THE COMPUTER SECURITY ACT OF 1987

HEARING

BEFORE THE

SUBCOMMITTEE ON
SCIENCE, RESEARCH AND TECHNOLOGY

AND THE

SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS

OF THE

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDREDTH CONGRESS

FIRST SESSION

FEBRUARY 26, 1987

[No. 8]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE
73-520 WASHINGTON : 1987

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

H701-54

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

ROBERT A. ROE, New Jersey, *Chairman*

GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
BART GORDON, Tennessee**
JAMES A. TRAFICANT, Jr., Ohio
JIM CHAPMAN, Texas
LEE H. HAMILTON, Indiana
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
TOM McMILLEN, Maryland
DAVID E. PRICE, North Carolina
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
DAVID E. SKAGGS, Colorado***

MANUEL LUJAN, Jr., New Mexico*
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, Jr., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID MORRISON, Washington
RON PACKARD, California
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, Jr., Virginia
LAMAR SMITH, Texas
ERNEST L. KONNYU, California
JACK BUECHNER, Missouri
JOEL HEFLEY, Colorado
CONSTANCE A. MORELLA, Maryland

Harold P. Hanson, *Executive Director*
Robert C. Ketcham, *General Counsel*
Regina A. Snyder, *Chief Clerk*
R. Thomas Weimer, *Republican Staff Director*

Subcommittee on Science, Research and Technology

DOUG WALGREN, Pennsylvania, *Chairman*

BUDDY MacKAY, Florida
LEE H. HAMILTON, Indiana
HENRY J. NOWAK, New York
DAVID E. PRICE, North Carolina
GEORGE E. BROWN, Jr., California
NORMAN Y. MINETA, California
TERRY BRUCE, Illinois
CARL C. PERKINS, Kentucky
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
TIM VALENTINE, North Carolina
JIM CHAPMAN, Texas
DAVID E. SKAGGS, Colorado
ROBERT A. ROE, New Jersey****

SHERWOOD L. BOEHLERT, New York*
PAUL HENRY, Michigan
CLAUDINE SCHNEIDER, Rhode Island
DON RITTER, Pennsylvania
SID MORRISON, Washington
D. FRENCH SLAUGHTER, Jr., Virginia
LAMAR SMITH, Texas
JACK BUECHNER, Missouri
CONSTANCE A. MORELLA, Maryland
MANUEL LUJAN, Jr., New Mexico***

Subcommittee on Transportation, Aviation and Materials

DAVE McCURDY, Oklahoma *Chairman*

DAN GLICKMAN, Kansas
BILL NELSON, Florida
TOM McMILLEN, Maryland
JIMMY HAYES, Louisiana
ROBERT A. ROE, New Jersey****

TOM LEWIS, Florida*
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, Jr., Wisconsin

---

*Ranking Republican Member.
**Resigned February 19, 1987 (H. Res. 89).
***Elected March 30, 1987 (H. Res. 133).
****Ex-Officio, voting member.

CONTENTS

WITNESSES

February 26, 1987: Page

Donald C. Latham, Chairman, National Telecommunications and Information Systems Security Committee [NTISSC], and Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Department of Defense 6

Lt. Gen. William E. Odom, Director, National Security Agency 41

Raymond G. Kammer, Deputy Director, National Bureau of Standards, accompanied by Mr. James H. Burrows, Director, Institute for Computer Science and Technology, National Bureau of Standards 75

Jack Simpson, president, Mead Data Central, Inc., accompanied by Mr. Kenneth Allen, senior vice president, government relations, Information Industry Association; Ms. Cheryl Helsing, information security manager, BankAmerica Corp. and chairman, Data Security Committee, American Bankers Association, and Mr. Geoffrey Turner, communications security manager, BankAmerica Corp 93

Jerry Berman, chief legislative counsel, American Civil Liberties Union, Washington, DC; Mr. John Richardson, chairman, Committee on Communications and Information Policy, the Institute of Electrical and Electronics Engineers, Inc., Washington, DC; and Mr. David Pronko, president PE Systems, Inc., Alexandria, VA 146

APPENDIX

Statement of Lee Neuwirth, vice president, Product Planning, Cylink 192

Statement of the American Library Association 203

THE COMPUTER SECURITY ACT OF 1987

THURSDAY, FEBRUARY 26, 1987

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY, SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY, AND THE SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS,
Washington, DC.

The subcommittees met jointly, pursuant to notice, at 2:07 p.m., in room 2318, Rayburn House Office Building, Hon. Dave McCurdy (chairman of the Subcommittee on Transportation, Aviation and Materials) presiding.

Mr. McCURDY. We are pleased to be joining our colleagues today from the Subcommittee on Science, Research and Technology for the purpose of hearing a cross-section of views on H.R. 145, the Computer Security Act of 1987.

As many of you know, this bill is very similar to a bill, H.R. 2889, reported jointly by this committee and by the Committee on Government Operations last year. The reason for that bill was a widespread view that something needed to be done to provide better protection for the information stored and processed in Federal Government computers, particularly unclassified information.

Hearings held over the last several years show that the Government has become highly dependent on computers to provide many essential services. For example, computers and the communications networks that connect them are integral to the life-critical air traffic control system. They allow the transfer of billions of dollars around the country each day. And computers store and maintain all kinds of personal information on our citizens.

Yet despite the incalculable value of much of this information, we found that it was vulnerable to unauthorized disclosure, fraudulent manipulation, and abuse.

The consequences of this situation ranged from financial losses as high as $1 billion per year, according to one government study, to invasions of privacy and to compromises of national security.

The probiem is clear. Virtually everyone agrees, better security and privacy protection are needed. The challenge that we face is to fashion a solution that balances the concern for efficiency with the fear of undue restrictions on the flow of information. We want a comprehensive solution that we can afford, that makes full use of the expertise residing in both the Government and the private sector, and that is compatible with safeguarding our fundamental freedoms.

The bill before us offers one way of meeting these goals. We will also be hearing much about the National Security Council approach, as embodied in National Security Decision Directive 145.

I believe we will hear an excellent sampling of opinion today as to the advantages and disadvantages of both approaches. I am hopeful we will be then able to sort out the essentials and agree upon a formula for dealing with a serious government problem.

Today our witnesses first will be Donald C. Latham, Chairman of the National Telecommunications Information Systems Security Committee. He is Assistant Secretary of Defense for C-Cubed-I, which in the armed services and intelligence language, is Command, Control, Communications and Intelligence.

Then we will have Lieutenant General William E. Odom, who is Director of the National Security Agency; Mr. Raymond Kammer, Deputy Director of the National Bureau of Standards; Jack Simpson, President of Mead Data Central, Inc.; Cheryl Helsing, Information and Security Manager of BankAmerica Corporation; Geoffrey Turner, Communications Security Manager, BankAmerica; Jerry Berman, Chief Legislative Counsel, American Civil Liberties Union; and John Richardson, Chairman, Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers, Inc.; and David Pronko, if that's pronounced correctly, President of PE Systems, Inc.

Needless to say, that's quite a witness list. We are going to try to proceed as quickly as we can today and give each an opportunity to present their views and also provide an opportunity for members to query each of the witnesses.

We understand, since we're out of session already today, I'm sure many members have already departed, but there will be, I think, Mr. Lujan, the ranking committee member on Science, Space, and Technology, and we have a number of members jointly from the SRT subcommittee that will be joining us.

At this point, I would like to recognize one of the principal authors of the bill, H.R. 145, the gentleman from Kansas, Mr. Glickman.

Mr. GLICKMAN. Thank you, Mr. Chairman. And I ask unanimous consent to put my entire statement in the record.

Mr. MCCURDY. Without objection, it is so ordered.

[The prepared statement of the Honorable Dan Glickman follows:]

HON. DAN GLICKMAN

FEBRUARY 26, 1987

H.R. 145
THE COMPUTER SECURITY ACT OF 1987

I WANT TO THANK THE CHAIRMEN OF BOTH SUBCOMMITTEES FOR CALLING AN EARLY HEARING ON THIS IMPORTANT ISSUE. I BELIEVE THE RECORD WE HAVE COMPILED OVER THE LAST FOUR YEARS SHOWS A CLEAR NEED FOR BETTER PROTECTION OF UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT COMPUTERS.

AND YET WE MUST USE EXTRAORDINARY CARE IN DECIDING EXACTLY HOW WE ACHIEVE THIS PURPOSE. A FUNDAMENTAL AMERICAN RIGHT -- OUR FREEDOM OF ACCESS TO INFORMATION -- IS INEXTRICABLY INVOLVED AND COULD BE COMPROMISED IF WE SELECT THE WRONG APPROACH.

I APPLAUD THE NATIONAL SECURITY COUNCIL FOR FINALLY TAKING ACTION TO FOCUS THE GOVERNMENT'S EFFORT. I WORRY, HOWEVER, THAT ITS NATIONAL SECURITY DECISION DIRECTION 145 AND THE RESULTING "POLICY FOR PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED SYSTEMS" -- THE SO-CALLED POINDEXTER MEMORANDUM -- RUNS THE RISK OF JUST SUCH A COMPROMISE.

I WOULD BE FUNDAMENTALLY UNCOMFORTABLE WITH ANY DIRECTIVE THAT AFFECTED VIRTUALLY ALL CIVIL AGENCIES OF GOVERNMENT AND THAT HAD BEEN ISSUED WITHOUT ANY PUBLIC COMMENT. BUT DIRECTIVES, SUCH AS THESE, THAT POTENTIALLY IMPACT OUR BASIC VALUES IN THIS COUNTRY MAKE ME PARTICULARLY NERVOUS.

THE BILL BEFORE US TODAY OFFERS AN ALTERNATIVE. I WOULD NOT CONTEND THAT THE VERSION WE HAVE TODAY IS PERFECT OR THAT WE CAN'T WORK OUT A COMPROMISE. BUT I DO FEEL STRONGLY THAT ITS BASIC CONCEPT -- CIVILIAN PREEMINENCE IN DETERMINING STANDARDS FOR PROTECTING UNCLASSIFIED INFORMATION -- IS A BETTER WAY.

MR. CHAIRMAN, I LOOK FORWARD TO THE TESTIMONY TODAY. I FEEL THE ISSUE WE FACE IS EXTREMELY IMPORTANT. AND I BELIEVE THE MIX OF OPINIONS WE ARE GOING TO HEAR WILL BE VERY HELPFUL IN GUIDING OUR ACTIONS.

Mr. GLICKMAN. I thank you for calling this hearing, and I believe the record we have compiled over the last four years shows a clear need for better protection of unclassified information in Federal Government computers. And yet we must use extraordinary care in deciding how we achieve this purpose. A fundamental American right—our freedom of access to information—is inextricably involved and could be compromised if we select the wrong approach.

I applaud the National Security Council for finally taking action to focus the Government's efforts; however, I worry that its directive and the resulting policy for protection of sensitive, but unclassified information, the so-called Poindexter Memorandum, runs the risk of creating an enormous problem for the Government.

I would be fundamentally uncomfortable with any directive that affected virtually all civil agencies of government and that had been issued without any public comment. Directives such as these, which potentially impact our basic values in this country, make me nervous.

For this reason, Congressman Brooks and I introduced a bill last year, which made it at least through consideration by the House, where we did not get two-thirds on its extension, but offered an alternative which essentially gave the National Bureau of Standards authority to manage computer security functions in the civil agencies of government for non-sensitive information.

The point of this bill, what we tried to do is, the people who have records, Social Security, the Veterans' Administration, all of the assortment of government computers, need to be assured that those records are properly protected and that there are adequate computer security safeguards.

But the basic concept of this bill, civilian preeminence in determining standards for protecting unclassified information is the heart of what we are trying to do, not military preeminence, nor do we want to get into military-related issues.

I don't think necessarily that this bill can't be compromised, but I think the basic concept of civilian preeminence is one that should not be compromised, particularly as it relates to civilian agencies.

Thank you, Mr. Chairman.

Mr. MCCURDY. Thank you, Mr. Glickman.

Mr. Latham, Mr. Secretary, since you have appeared before a number of committees quite often, I think you know the standard procedure. We'd like to have you summarize your statement as best as possible, and then we will include your formal statement in its entirety in the record, and we would like to, because of the number of witnesses, proceed as quickly as possible, in order that there be a fair exchange here with questions.

As you can tell by the members present, there is some direct interest, and I think the discussions should prove to be lively and informative.

At this point, Mr. Latham, you are recognized for your statement.

STATEMENT OF DONALD C. LATHAM, CHAIRMAN, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE [NTISSC], AND ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE, DEPARTMENT OF DEFENSE

Mr. **Latham**. Thank you very much, Mr. Chairman.

As you mentioned earlier, I am also the Chairman of the National Telecommunications and Information Systems Security Committee, and in that light, I think the statement for the record is a very broad statement, and I would encourage people to read it, because there appear to be a number of misunderstandings about what the National Security Decision Directive 145 does and doesn't do, what powers the committee I chair has and so on and what the Steering Committee that runs the whole show really has under its authority. So I would encourage people to look at this and try and help understand.

As you did mention, last year we had H.R. 2889. I testified in front of Chairman Brooks' committee on H.R. 2889. This bill, H.R. 145, is very, very similar to H.R. 2889 of last year, and our position last year was that we felt that the bill, as written last year, and the bill, H.R. 145, as currently written this year, is largely unnecessary. However, I think as the opening statements of Mr. Glickman and others have indicated, we are actually much closer on this than would be indicated, in that we are all concerned about the security of information. We are very concerned about a large body of information that is, in fact, unclassified, but sensitive information that resides in computer systems and in memories and in other machines that are vulnerable to unauthorized access and so on, and we all, I believe, are very interested in seeing how we can best protect that within the proper framework of access to information by people who should have it and so on.

So there is a basis, I think, for coming up with some legislation that we could all—agree with, and I will also agree that there is an awful lot of work to be done, and there is certainly a very good relationship now between NSA and NBS, and I think that there could be an even expanded relationship. There's work aplenty for both of us, and so maybe it's possible to work a set of legislation that we could all live with.

The concern I have primarily is that this other piece of paper that was issued by Admiral Poindexter as a statement of what is sensitive, but unclassified is, in fact, very close in definition, almost identical, to what is in H.R. 145 in terms of the definition. However, the problem with that is, it's been so misunderstood as to exactly what we have intended or not intended with that particular policy statement—and it was nothing more, in fact, but an awareness policy statement—and unfortunately it's been construed that somehow the Department of Defense or the National Security Agency or some other agency now has authority to actually impose some sort of controls over these unclassified data bases, and that is simply not the case.

There are people who have claimed that this—a combination of NSDD-145 and the policy statement from the NSC—somehow gives the right to restrict public access to not only classified information, but also to any civilian agency information which it considers "unclassified, but sensitive," unquote.

That is simply not the case. The Department of Defense, in particular, nor NSA, again, nor any other agency is empowered to do anything about that situation. The fact is that the agency head or the owner of the bank, for example, or the owner of the newspaper or whoever owns the data, the manager of the data, determines, in their particular empire, what is sensitive unclassified information. They do the determination on their own. If they want to go ask some experts for some opinions, they certainly, obviously can do that. But the ultimate determination resides with the agency head.

So once they've decided, the second thing the agency head can do is to go to again some experts and say, "Okay, if I need to protect this information, how is the best way to do it?" That agency head or that owner of the bank or that particular library or whatever then can take the necessary steps to go to the civil sector and procure whatever security equipment or procedure or so on that they would like to put on to their data.

It is not a new classification category of information. That's important. And it is also very important—and it came up in the hearing this morning—that somehow people believe that once somebody has declared that there is a body of information that's sensitive, but unclassified, somehow the Department of Defense or, worse yet, NSA somehow would come in and put a lock on it and keep the key. That's nothing further from the truth.

Again, the agency head is the determination person of the classification of the material, if any, or is it just unclassified and sensitive, and if so, then they make the determination of how to protect the information, if they so desire to do it.

And I think that if we could get that very, very important point straight, I think a lot of the worry over this material would disappear, and then we can get back to the, I think, important business you're trying to do, and that is, how do we structure the Federal Government to best manage information security.

And I'll just leave it there, Mr. McCurdy, and answer any questions I can, sir.

Mr. McCurdy. Well, thank you, Mr. Secretary. And I apologize. I am fighting a terrible cold today or flu bug or something.

I think in narrowing the issue, it appears that—I know last year in the debate on the floor, one of the principal points of contention was in the use of the term "sensitive," the definition of the term, and who was to make that determination, and then again, who was to control that data.

What are the principal differences, in your opinion, between yourself and the relevant agencies that you represent in the definition of "sensitive information" that is contained in the bill, H.R. 145?

Mr. Latham. There is virtually no difference between the two definitions, the one that was issued by the National Security Council and the definition that's in the bill.

I might add that the definition in that policy document that Admiral Poindexter signed was discussed within the Federal Government across all the 21 agencies that belong to the NTISSC Committee that I chair. It was, in fact, hotly discussed, every word, everything. Various lawyers looked at it. It was not something that was done in any secret way or anything, and it was an agreed community definition.

And at the same time, in a point Mr. Glickman made earlier about the civilian control here, there is in NSDD–145 a Steering Group. The Steering Group is chaired by the Assistant to the President for National Security Affairs and then is composed of all civilians from the various cabinet level departments that are on the Steering Committee—Treasury, Defense, State and so on—so that there is, in fact, at the very top of the NSDD–145 structure a group of cabinet level civilians who actually operate the mechanisms that are laid out in H.R. 145.

Then in the committee that I chair, we have 21 agency members. We have a large number of observers, a total of 37 different agencies represented there by either observers or members, a majority of which, the overwhelming majority of which are, in fact, from the civil sector—I mean, the civilian sector of the Federal Government. So that the civilian side is well-represented, as I think it should be.

So the definition that we have in that policy document was one that all of these people participated in and agreed to.

Now the determination of what is sensitive is again back to some agency head. Let's take the Department of Agriculture. They may have a set of information on crop forecasting that could, in fact, affect the commodities market residing in a computer system. That might be deemed by the Secretary of Agriculture to be sensitive, but unclassified information. That's his determination to make.

In the case of the Secretary of the Treasury, he might determine that IRS records, information that's generated by the Coast Guard on narcotics and drug trafficking, things of that nature, which is unclassified in a strict national security sense, but is sensitive, should be protected in some way. He would make that determination again.

So it's on a case-by-case basis made by the agency head or in the case of the civil sector, truly out in the private sector, the owner of the bank, the director of the bank, whoever it might be, that has control of the bank's data base.

Mr. **McCurdy**. Where do you see, as concise as possible, the stumbling blocks from acceptance within the Defense Department and the National Security Agency, as it pertains to this particular bill?

Can you just list—and if you need, would you provide for the record—I guess maybe a better question is, do you believe that the bill, as presented, with some perhaps recommended changes or suggestions that you have, would that be a vehicle that would be acceptable from your standpoint to address this problem?

Mr. **Latham**. Yes, sir. I have taken the bill and personally marked it up to add some words here or there, and I'll be very glad to share that marked up copy with you. It is, in fact, in my judgment, a very minor marking up, and basically what it does, it says there is a role for the National Bureau of Standards, working with the National Security Agency's Computer Security Center that was established under NSDD–145, and especially there is a major role for NBS in the area of this unclassified, but sensitive information in helping set standards, in training, in education, a number of roles.

There's plenty of work for them to do, and I will be very glad to submit for the record a copy of this—Don Latham's marked up copy of this as the Chairman of NTISSC, and I think if you look at that, I think from that we could negotiate a bill that would be, I think, very satisfactory to both parties.

Mr. McCURDY. I appreciate that, and I think that's very constructive, if you will submit that for us.

Mr. LATHAM. Yes, sir.

Mr. McCURDY. One last point before I turn to my colleagues, which relates to duplication of effort, and I know last year during the debate, there was some concern that, in effect, we were going to be having two separate agencies. But your last comment that there's plenty of work for both and that there could be clearly delineated functions without major duplication problems; is that accurate?

Mr. LATHAM. Yes, sir, I believe so. Let me give you an example.

The National Bureau of Standards, as the name says, is the federal agency charged with developing and promulgating various standards including, in this case, they have done this in the past on various computer systems—issues. The important thing is that whatever standard is generated, that it be a standard such that we assure that the technique, or whatever it is that's going to be implemented as a result of that standard, does not result in systems that won't interoperate with each other, or completely different technical approaches, so that we have an integrated approach to this computer security thing, such that we're not off inventing with two different R&D programs, two different ways of doing it because we don't have a set of standards that we have worked together, so the way I would see this working is, that NBS and NSA's Computer Security Center and the other members of the NTISSC community, the 21 other agencies, working together can develop standards that we could agree to, and make sure that they're in a command control communications terminal, that they're interoperable, and that we've got standards that are good across the whole spectrum. So I think there is plenty of room, and plenty of work that could be shared that way.

Mr. McCURDY. Thank you, Mr. Latham. Mr. Glickman.

Mr. GLICKMAN. Thank you.

Mr. Latham, first of all I want to congratulate you as well as the National Bureau of Standards for, I think, changing their position from last year or taking a much more enlightened position and this is something that should be able to be worked out, and I really don't have any questions for you, but I thought I would then share, because the issue has been going on for a long time, what led to all of this.

This was not an attempt to have a confrontation with the National Security Council. This was an attempt to ensure that people who had information stored in Federal computers went to sleep at night, knowing that that information couldn't be manipulated or stolen. That whether it was in the Veterans' Administration or the Social Security Administration or in banking systems in this country, it was an attempt to ensure that people who relied on Federal computers to transfer their monies around, or to transfer electricity on the electric grid or transfer their bodies via the air traffic control system, would know that those computers were properly protected, so that people couldn't come in and wreak havoc on their lives.

We had a series of hearings on this point. We brought in one of the hackers from Milwaukee. We showed a clip from the movie "War Games," and we talked with people all over this country, and the GAO came in and did a report and they said there was a serious national problem here.

The Inspector General of HHS came in, Mr. Kussero, and you may know him, he's the man who is prone to tell it like it is, and he basically said that very few Federal agencies had done anything whatsoever with respect to protecting information in computers, changing passwords, training people, doing anything along those lines.

Nobody wants to get into classified information or jeopardizing national security. That's not my goal and that's ridiculous to do that anyway.

The goal we saw was a national problem here, and how to deal with that goal, what was the best way to deal with it. We put up this bill because we felt the National Bureau of Standards had a long history of dealing with computers security and ought to take the lead in training and maybe developing standards for the private sector and that kind of thing.

Then NSA and you all came along with Directive 145, and I think that caused people concern. Twelve out of, I think, the 22 members of the group were military. It had a military focus to it. For the most part, there were not all the agencies, civilian agencies of the government, represented.

There was the feeling that you might—and the Department of Defense has a legitimate reason to restrict information flow—that you might in fact restrict information flow in non-government computers or non-military computers. You might somehow prevent the unrestricted flow of access to information regarding personal records, and recognizing that the DOD is perceived as having a track record of attempting to restrict information flow, and I don't say that entirely in a pejorative way, we felt that it would be inappropriate to give you the authority to manage all of these systems. And, frankly, the civilian agencies were not very happy about it either.

At the same time I think it's appropriate to try to work out a compromise because we have a problem here, a serious national problem, and it's going to get worse as we expand the use of data processing systems control.

I am just glad to know that you are willing to work with us on this kind of thing, and I think it's appropriate that this, if possible, can be settled without unnecessary delay or unnecessary friction.

Mr. Latham. Yes, sir.

I might add that in your help to the other agencies, one of the things we've discovered on the NTISSC in meetings, and one of the things before the steering committee now is a national funding mechanism to fund for these necessary protections in these agencies who find a very difficult job of getting the priority to their secretaries or whatever they happen to be in those agencies to buy even the minimal kind of protection for their systems, so we do need some mechanism there to do that because it is a serious problem, as you say.

Mr. GLICKMAN. I just would finally—I thank you again for your testimony and it is obvious that particularly as a result of recent events in the world, including the release of the Tower Commission Report today, that there is a skepticism, a healthy skepticism, about national defense agencies having control of anything which would affect civilian—truly civilian aspects of their lives.

Mr. LATHAM. Yes, sir.

Mr. GLICKMAN. I think that this debate is useful as we try to develop a compromise, realizing of course, that people still don't want big brother watching.

Mr. LATHAM. Absolutely. I understand. Thank you.

Mr. MCCURDY. The distinguished gentleman from New Mexico, Mr. Lujan.

Mr. LUJAN. Thank you, Mr. Chairman.

I guess to follow up on that, and that is really the central question. We started out by having a bill that would train the civilian federal work force, and then we all of a sudden, you know, the whole thing spreads out, and there's fears all over the place that if the Department of Defense or National Security Agency, or anybody with military background gets a hold of something, that it's going to stamp a classified thing on it whether it's libraries, or whatever, and that other people aren't going to be able to get at it, and I don't care what we do, we're not going to get away from those arguments because—well, because of different interests that are involved.

But just to try to do that, is there some mechanism, if it does stay where it is, under the Directive 145, is there some mechanism to prevent you from classifying, putting the big classified stamp on everything that comes in?

Mr. LATHAM. Yes, I'm glad you raised that, sir, because that seems to be a fear of people and I can't quite put my hand on it as exactly why they feel that way.

In particular, in the NTISSC meetings that I chair, in which these other agencies are there, and the observers are there, that fear has not come up and been raised, and in the Subcommittee meetings, and so on, there has been a lot of discussions about various policy issues, but the fear of the Department of Defense or NSA going over and saying to the Department of Health or the Department of Agriculture, or someplace, and saying your data base is hereby stamped whatever, is incredible. We simply have no authority whatsoever to do that, as the NTISSC, let alone the Department of Defense.

The Directive 145 does not permit the NTISSC to go over and tell some agency, your data base is classified. In point of fact, it says that the Department of Agriculture, the Secretary of Agriculture, or whomever he might appoint, is the authority for deciding what in his domain would be considered sensitive and unclassified, or perhaps confidential, or whatever level of classification he would put on it.

Now he can come to some people and ask for advice, and one of the things that we've been doing over the last year—two years very intently, is we've been sending out videotapes, various pamphlets and brochures, sending briefing teams out to talk to people to let them know about what type of information is available, what type of security devices, procedures are available, but in no way attempting to ever come in and do an audit, so to speak, on somebody's data base.

Now there have been stories about various agencies visiting owners of unclassified data bases in the commercial sector, as well as the NTIS people in commerce, and apparently some of those visits took place. Not to go in there and say, you ought to classify your data base, but to go in there and understand who uses the data base, where is it going, and what is going into it, where does it go out of, rather than try to put any classification on it.

For example, the NTIS is fed largely from two sources, the Department of Energy and the Department of Defense. We are the biggest contributors to that data base. About 75 percent of the users of NTIS are in fact small businesses and the scientific community and the universities and so on. We don't want to cut that information off.

What has been of concern, in the Air Force study that was done looking at protecting data bases, is that there is a hemorrhage of U.S. technology going to everybody. Not just the Russians, but a lot of people who would consider themselves our friends, and is there any way to stem that to some extent, without inhibiting the free exchange of scientific information and so on.

It's a very fine line you have to walk, but the classification of that data base in NTIS is up to the guy who puts the information into it. If DOD submits a report to NTIS and said it's unclassified, or DOE or whomever, that's their responsibility to make that classification and not NSA or Department of Defense.

Mr. LUJAN. You have a steering group, let's see, about seven or eight people——

Mr. LATHAM. Yes, sir.

Mr. LUJAN. Seven or eight people that run this thing.

Mr. LATHAM. Yes, sir.

Mr. LUJAN. One of the things that always interests me about putting things in the DOD is that you are the ones that have the bucks. That's always—and whether—not National Science Foundation, but NBS would have the money to do all of that, though I suppose you could appropriate the money.

Mr. LATHAM. Well, I think the Deputy Secretary of Commerce testified this morning in front of the Brooks Committee that the number of people they believe that it would take to do their portion of the work would be on the order of 20 people. That's a modest effort, and probably affordable within the Commerce budget.

Now we have, as you know, a research and development program and some 300 people growing to approximately 350 authorized in the National Computer Security Center, so that it's not a gigantic thousands of people or anything like that. It's a modest effort.

Mr. LUJAN. The bill as it is now, H.R. 145, you have some concerns about weakening the data base?

Mr. **Latham**. No, sir. The concerns are more that the way the bill is currently written would end up building a duplicative structure and I believe with some minor wording changes, we can actually work out an arrangement where the NBS role is very clearly defined, and a very major role in this unclassified but sensitive information area, in setting standards, educating people, et cetera, and that's what we're concerned about, the way it's currently written.

Mr. **Lujan**. So, it's the duplication and not the security of the data that has you more concerned?

Mr. **Latham**. No, sir. Everybody is concerned about doing something about the security of information.

Mr. **Lujan**. You don't see any problem with the bill so far as the security is concerned?

Mr. **Latham**. No, sir; I don't. I have some suggested changes that I told the Chairman that I would be glad to submit to you for the record to show you, that I think some minor wording changes would even make the bill acceptable.

Mr. **Lujan**. What about if we let you handle, if we changed it, to let you handle all of the military things, and set up one just for the—as we started to do, just for the training of the civilian workforce?

Mr. **Latham**. I think that would be——

Mr. **Lujan**. That's duplicative.

Mr. **Latham**. I think it would be duplicative because—let me mention that it isn't just within the Department of Defense that there resides a great deal of classified information and extremely sensitive information.

The Department of Energy is an example, the Department of State, the FBI, Justice, Treasury, a number of other places, so that there is a need to have a uniform system and a uniform set of standards and somebody who you can hang and say, you're in charge of making sure that you get these standards, you get the devices, you have the education program and so on, from the most insensitive information all the way to the most sensitive, rather than have two complete separate agencies trying to somehow divide up that complex pie.

Mr. **Lujan**. What happens to you if you were to classify information that should be readily available that some other agency puts in? You get fired? You get shot? You get thrown out of the window?

Mr. **Latham**. I don't know any way to do it, frankly, but I guess what would happen is that the agency whose data were somehow classified without its authority could certainly raise Cain at the Cabinet level through their secretary, to the President, and get that reversed in a hurry, and through the Steering Committee.

Mr. **Lujan**. Thank you.

Mr. **McCurdy**. Thank you, Mr. Lujan.

We have two new members on the Committee this year that certainly hold a bright promise for a very substantive contribution, and the first is Mr. Price from North Carolina and Mr. McMillen from Maryland.

Mr. Price, the gentleman from North Carolina.

Mr. PRICE. Mr. Latham, I wonder if I could just question you briefly on a related matter. The Wall Street Journal carried a story on February 5th of this year concerning Defense Department efforts to block U.S. scientists from delivering papers on Government funded research, mostly on optics and composite materials, it said, in open sessions, and has restricted the circulation of unclassified research that it deemed sensitive.

I wonder if you could just—not having been in on previous Committee deliberations on this subject—I wonder if you could just fill us in a bit on the extent of those efforts, and the form that they've taken.

Mr. LATHAM. Yes, sir, I'll try. I believe that story relates to something that happened quite some time ago, and that there is an annual conference dealing with optics and electrooptic devices, and so on, in which a number of papers were submitted that had not been reviewed for clearance as to the sensitivity of the information in the papers and so on, and some of those papers were withdrawn from that particular conference. I think this happened 1-2 years ago.

More broadly, what we've been concerned about is that in certain areas of research, such as composite materials, such as optics and electrooptics, and all of the associated countermeasures and other techniques that you can do with very sophisticated optics today, are integral to so many very important initiatives within the Department of Defense and elsewhere, so we are attempting to make sure that while it may look to the uneducated eye, even though that the researcher may be a very brilliant person, that his particular piece of research, as it could be fit together in a puzzle by a trained analyst, can lead you from one story to another is pretty soon a capability.

For example, by watching the flow of scientific papers, in terms of the titles to the papers, short abstracts, where the work is done, the number of papers that are published, and so on, one can quickly glean where the key research centers are, which we attempt to find out in terms of other people, what is the level of sophistication of the research that they're probably engaged in, and as the research matures and you watch this for 1-2 years, you can quickly discern that it is very likely they've achieved some sort of a capability or they're aiming to that type of capability.

In fact, the Soviet Union watches the publication of their material extremely closely for exactly that reason and you'll find in some cases, Soviet literature all of a sudden disappears completely in certain areas.

So the trained intelligence analyst can take numerous—numerous pieces of unclassified information on various types of scientific papers and quickly glean things that you'd prefer that they don't. It's that kind of a story.

But in point of fact, in those areas that we're doing that kind of research, like composite materials, like optics, the people who are doing that work are in the large cleared for DOD or Department of Energy, or other agency clearances, and have a very free exchange at the classified level.

Mr. PRICE. Now, when you talk about this clearance, you're talking only about research that in some way DOD is supporting?

Mr. **Latham**. Well, it could be Department of Energy supporting it or some other agency could be supporting it, but in the large, let's stick to DOD. Yes, sir.

Mr. **Price**. What is the procedure for reviewing the range of research that might possibly be sensitive?

Mr. **Latham**. Well, the determination is usually made before the contract is awarded, be it to a university or to a research institute of some kind or to a company, whether or not that particular piece of research will be conducted at an unclassified or at some classified level and as a result, the material that he or she uses for the research and the access they have is accordingly as a result of that.

Mr. **Price**. Excuse me. DOD reviews not just its own research, but also in some systematic way, the research contracted by other departments?

Mr. **Latham**. No, sir. I'm just speaking to Department of Defense, Department of Defense contracts, and so a contract is let generally with the security classification on which that research will be conducted prior to the award of the contract. Now, it might be that at some point during the work on that contract, the researcher stumbles across some very important aspect and it's deemed necessary that he or she brings that information into the sponsoring agency in the Department of Defense, and it's determined, boy, you really stumbled onto something, this is important, we should in fact classify that information at some level, that could occur. So, an unclassified research program could in fact lead at some point to some classification.

Mr. **Price**. Well, the example you cite is one where the researcher himself would come to the department.

Mr. **Latham**. Yes, sir.

Mr. **Price**. Is there some kind of departmental initiative in this regard to monitoring?

Mr. **Latham**. Yes, sir, in the sense that let's say that the researcher would like to now present a paper at some conference, like this optics conference. The procedure is that they write the paper and send it in to the sponsoring agency. It's reviewed for classification and then sent back to the researcher to present. So, there is a check done to see that in point of fact, the paper is unclassified.

Mr. **Price**. So, you do systematically review papers being presented in the professional setting for their sensitivity?

Mr. **Latham**. Yes, sir, from Department of Defense sponsored contracts, not necessarily from other independent research efforts or anything like that.

Mr. **Price**. Well, I wonder if you could clear up the earlier reference then to research outside DOD?

Mr. **Latham**. Well, that's up to the agency that is sponsoring that research. Let's say that the Department of Energy, which as you know, performs several billion dollars a year worth of work for the Department of Defense, and some of it is very, very highly classified research work in nuclear weapons design, effects, and so on. It is a DOE, Department of Energy responsibility to ensure that those contracts are handled at the proper security level and reviewed for that, not the Department of Defense.

Mr. **Price**. DOD exercises no oversight with respect to that?

Mr. LATHAM. Well, we might advise them, if we happen to see something or if we're asked, but the contracts are let by DOE, managed by them, their laboratories are run by them. We do not get involved in telling them how to classify information. We have an agreement throughout the Government as to what generally should be secret, or top secret, and so on, and that's generally understood, so there's hardly any disagreements there on that.

Mr. PRICE. Thank you.

Mr. LATHAM. Yes, sir.

Mr. MCCURDY. The gentleman from Maryland, Mr. McMillen.

Mr. MCMILLEN. Thank you, Mr. Chairman.

Some of the concerns that I have regarding this issue, I guess I'm particularly sensitive to it in my district, we have a National Security Agency, and it has to do with being able to provide a unified coordinated approach to the problem. GAO testified at the Government Operations hearings last year that the definition of "sensitive information" in Poindexter's memo is too broad and is causing confusion among several agencies.

My question relates to how can we be sure that there is a—that the civil agency heads have a coordinated idea as to the criteria that apply when there wasn't any problem within their agency, so that there is a unified approach to this within the Federal Government?

Mr. LATHAM. Yes, sir. That's a good question, and I would point out that the definition of "sensitive but unclassified" that's proposed in H.R. 145 is very, very close, and I'd have to go back and check the exact wording as to what was in the Poindexter memo, but it comes down to a matter of judgment on the agency head, as to what he or she determines may be sensitive enough to want to protect. It runs from the rather mundane to something that's rather obvious.

I believe it would be generally agreed that things like IRS records, Social Security records, personal health records, things that people would not normally necessarily say were at all classified, really need some degree of protection against unauthorized access or manipulation.

As you know, one of the hackers a couple of years ago got into a hospital information system and manipulated and destroyed some records. That's the kind of thing you really would like to try and protect against, and so it's a judgment call, and in the case of some administrator of some agency that's not familiar with some of the various threats to this kind of information and so on, they can go to the National Bureau of Standards perhaps, or to the National Security Agency's Computer Security Center, and ask for a professional judgment as to what the degree of protection ought to be afforded to that information, and they'll give them that judgment.

Mr. MCMILLEN. I guess because I think some people might view prudent steps as one thing and others may view it entirely different, so they do have some back drop really to go to, to look at.

The other question that I really—or the other angle that I'm interested in has to do with what is happening internationally with regard to the Japanese, the French, where there is truly a proliferation of computer services.

Mr. LATHAM. Yes, sir.

Mr. McMILLEN. What is happening in terms of pulling information, sensitive information from those countries?

Mr. LATHAM. There is—it's rather interesting that you asked. I happened to come across an article today about USSR non-bloc access to Soviet data bases. It turns out the Soviets have four rather large data bases on-line, you can dial up on a telephone through Finland or Austria, and get into the Soviet data bases, and allegedly get, I would presume, unclassified Soviet information on scientific and engineering things, and that's rather interesting, all the different places you can apparently dial into. And this is true in France and Germany. There are a large number of data networks and access methods over there.

I think everybody is now resigned to the fact that to, in fact, encourage commerce and trade and technology sharing, that you're going to have to do something about continuing to have these data bases available to people. Right today you can access and others do, our NTIS data base and pull out hundreds and hundreds of documents all the time and I just don't know any way that is sensible to restrict that or you're going to end up back in a type of country you don't want to live in.

Mr. McMILLEN. I'm proud to see folks are opening their data bases around the world, but——

Mr. LATHAM. I'm not sure they are, but there are people who would allege that.

Mr. McMILLEN. My concern is that for the past six years we've seen these electronic data bases grow eightfold, and I'm concerned as to just the effect of the proposed bill. There's no question they're needed.

Mr. LATHAM. But we've done a study on that. Take NTIS, which is a commerce operated data base service. As I mentioned earlier, they sell some 75% of their sales on that, which amount to about $30 million a year, they told me the other day, to small businesses, by definition of small businesses, and then universities, scientific people, and so on, and we, the Department of Defense, and Department of Energy, are the big inputers of data into that.

I think that you just have to be, on the front end, very careful of what you put in. It's back to an article on optics or an article on composite materials. If the person who owns that article, that is the sponsoring agency decides that that material if aggregated and so on over a period of time would in fact be considered sensitive, then they should not input it into the data base and they can put it in the Defense Technical Information Service, and we could then make it available through that mechanism, which is a little more protected. You've got to be careful what you put in, if you don't want to lose it.

Mr. McMILLEN. One last question, in that Poindexter memo, the CIA Director has the responsibility for identifying sensitive information. Can he intrude into the private sector, direct a private entity?

Mr. LATHAM. No, sir, and let me correct something. I don't know of any authority for the Director of Central Intelligence or in particular, the Director of CIA to identify what is sensitive except in his agency. He has the full authority within the Central Intelligence Agency, of course, to decide which of his data bases he believes are sensitive but unclassified and should it be afforded some degree of protection. But he cannot come over to the Department of Defense, in particular, for example, or Department of Energy, or any other place, and say, your data base such and such is such and such classification. He does not have that authority.

Mr. **McMillen**. Thank you.

Mr. **McCurdy**. Point of clarification, in the Poindexter memo, in Section four, responsibilities, it states that "The Director of Central Intelligence, shall, in addition, be responsible for identifying sensitive but unclassified information bearing on intelligence sources and methods, and for establishing the system security handling procedures and the protection required for such information." Intelligence sources and methods, that's a totally different——

Mr. **Latham**. Yes, sir, that's a very specific, narrow area for his responsibility. That's correct.

Mr. **McCurdy**. Secretary Latham, thank you very much. We look forward to seeing your—oh, I'm sorry. The gentleman from Pennsylvania.

Mr. **Walgren**. I have no questions.

Mr. **McCurdy**. Thank you. We look forward to receiving those suggestions as far as a mark-up on that bill, and appreciate your attendance today.

[The prepared statement of Mr. Latham follows:]

STATEMENT
BY
DONALD C. LATHAM
ASSISTANT SECRETARY OF DEFENSE
COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE
AND
CHAIRMAN
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY
COMMITTEE
CONCERNING H.R. 145
BEFORE THE
SUBCOMMITTEE ON
TRANSPORTATION, AVIATION, AND MATERIALS
AND THE
SUBCOMMITTEE ON
SCIENCE, RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES
FEBRUARY 26, 1987

Mr. Chairman and members of the Subcommittee:

Thank you for the opportunity to appear before you and to testify on H.R. 145, the "Computer Security Act of 1987." I commend you, Mr. Chairman, and the other members of Congress who have displayed such a well-deserved interest in the field of information security. Also, I want to extend to you my appreciation for your having provided such outstanding leadership in this area.

However, while I heartily endorse the intent of H.R. 145, especially because it provides Congressional support for computer security training and awareness, I view the overall bill, as currently written, as unnecessary because we believe we already have the necessary statutory authorities to carry out a more than adequate computer security program throughout the Federal Government, and to assist the private sector in this vital area.

National Security Decision Directive (NSDD) 145

In my view, the proposed bill, as currently written, is designed to address a problem which the Administration recognized some years ago, and which is already being addressed under a management structure created by the President under National Security Decision Directive 145.

I am well aware of criticisms that have been levied against NSDD 145, and some of the policies that have flowed from it and its management structure. These criticisms have appeared not only in Congressional reports, hearings, and floor debate, but in the press as well. I would like, therefore, to discuss those criticisms for the record.

NSDD 145, for example, has been called "an unprecedented expansion of the military's influence into our society . . . ." Critics have also claimed that it would give the Department of Defense the power to "control the access to not only classified information, but also to any information which it considered sensitive." Nothing could be further from the truth.

First of all, NSDD 145 establishes a six-member steering group [see Table #1] to oversee implementation of the directive. The steering group consists entirely of civilian members of the President's Cabinet (the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, and the Director of Central Intelligence), and is chaired by the Assistant to the President for National Security Affairs.

The directive also establishes a 21-member interagency National Telecommunications and Information Systems Security Committee (NTISSC) [see Table #2], which I chair. A majority of the NTISSC's membership (13 of its 21 members) are from civilian agencies, and even the military departments represented on the committee are, of course, headed by civilian secretaries, in keeping with the American tradition of civilian control of the military.

Most of the Committee functions are handled at the operating level by the NTISSC's two permanent subcommittees: the Subcommittee on Telecommunications Security (STS) [see Table #3], currently chaired by Mr. William A. Bayse, Assistant Director, Technical Services Division, FBI; and the Subcommittee on Automated Information Systems Security (SAISS) [see Table #4], currently chaired by Mr. Patrick R. Gallagher, Jr., Director, National Computer Security Center.

Considerable effort has been expended over the last year, particularly by the Subcommittee on Automated Information Systems Security of the NTISSC, to expand the involvement of civil sector Federal agencies in NSDD 145 activities. In the past year, the Department of Agriculture, the Department of Education, the Department of Health and Human Services, the Department of the Interior, the Department of Labor, the Office of Personnel Management, and the Veterans Administration have all become directly involved in the SAISS as observers. Only one Cabinet department--HUD--remains to join, and we hope to have it participating very shortly.

The STS and the SAISS have the same generic responsibilities, one focusing on COMSEC (including TEMPEST), the other on computer system security. The two subcommittees work closely together, sharing subcommittee representatives, in some cases, and joint working group members. The major responsibilities of the subcommittees range from developing policy recommendations, developing guidelines, and developing standards for securing telecommunications and automated information systems; to developing an annual assessment on the status of telecommunications and automated information systems security in the federal government.

The Annual Information Security Assessment Report

In order to assist in the development of the Annual Report, we have established the National Information Security Assessment Center and the National Computer Security Center to assess security aspects of government telecommunications and automated information systems, and to evaluate the vulnerability of these systems to interception and exploitation. Specifically, the Annual Report assesses the security posture of the total U.S. Government telecommunications and automated information systems which process classified and/or sensitive information. The Annual Assessment Report is forwarded by the Chairman of the NTISSC to the Chairman of the Systems Security Steering Group (the Assistant to the President for National Security Affairs) for review and comment by the Steering Group.

The first annual assessment, issued in August 1985, made a series of recommendations to ensure adequate telecommunications and automated information systems security resources could be made available to achieve the objectives of NSDD 145. Since the issuance of that report, significant progress has been made towards fulfilling those recommendations. Specifically, the recommendations focused on the development of national policy in the following areas: (1) a policy defining sensitive information; (2) a policy defining a minimum level of protection for automated information systems processing classified and/or sensitive information; and (3) a policy establishing a national information systems security education, training and awareness program. The first annual report also specified the need for guidance in fostering an aggressive R & D program to encourage the development of products to effectively enhance the protection of information systems.

The second annual assessment, sent to the Chairman of the Steering Group in the summer of 1986, highlighted the most significant vulnerability in U.S.telecommunications, which is the predominant use in the Federal Government of the unprotected telephone. We believe that the single best source of intelligence to our adversaries is the common telephone.

The second most serious finding in the second annual assessment focused on the need for much more stringent hardware and software controls and security measures to ensure the protection of sensitive and classified information stored, processed, or transferred by automated information systems. The report recommended that until trusted systems can be incorporated into the marketplace and the government inventory, federal government departments and agencies should protect information processed in automated information systems and networks using security features identified by the National Computer Security Center. To accomplish this goal, the National Computer Security Center has vigorously endeavored to further populate the Evaluated Products List (EPL) with approximately two dozen new security products by the 1988/1989 time frame. These same commercially available products can be employed by the private sector as they deem necessary. Advice is freely provided to any sector as to the degree of security, use, and other features of the EPL.

Policy Initiatives

A permanent, government-wide mechanism for overall increased funding for Federal information systems security has been identified as a critical initiative for assuring the long-term security of telecommunications and automated information systems. The NSDD-145 Steering Group is examining a national policy to provide the mechanism for an improved systems acquisition process, ensure government-wide participation in the program and budget process, and establish the funding means to effectively execute responsibilities delineated in NSDD 145. Such a policy will ensure a shared national responsibility for all Federal agencies in safeguarding telecommunications and automated information systems.

The NTISSC has also actively pursued the promulgation of national issuances to ensure that telecommunications and automated information systems are secured using national standards and policies in consonance with NSDD 145 and Federal statutes.

The NTISS Issuance System promulgates policies, directives, instructions, and advisory memoranda that apply to all federal departments, agencies, and organizations within the Executive Branch. NTISS Issuances must be fully coordinated with the

Committee prior to promulgation. Policies are promulgated by the Executive Agent; directives are promulgated by the Executive Agent, or the Chairman, NTISSC, when so designated by the Executive Agent; and Instructions and Advisory Memoranda are promulgated by the National Manager.

On 18 November 1985, the National Manager promulgated NTISS Advisory Memorandum (NTISSAM) COMPUSEC 1/85, entitled Advisory Memorandum on the Department of Defense Trusted Computer System Evaluation Criteria. This advisory memorandum was issued to acquaint federal departments and agencies with the Criteria and to afford them a one-year trial period in which to evaluate the applicability of the Criteria against the requirements and environments of the individual organizations. In close coordination with the SAISS, the National Computer Security Center has conducted an aggressive Criteria familiarization program designed to acquaint approximately 70 government organizations with the Criteria and to demonstrate the utility of technical solutions as one basic aspect of information security.

The NTISSC is currently reviewing a draft national policy, entitled Controlled Access Protection, establishing a minimum level of technical protection for automated information systems operated by the government. This draft policy establishes a requirement to implement a minimum level of technical and operational protection for automated systems accessed by more than one user when those users do not have the same authorization to access all of the classified or sensitive categories of information stored and processed by the automated information system.

The NTISSC is also considering a draft national directive entitled Telecommunications and Automated Information Systems Security Education, Training, and Awareness. This draft directive establishes the requirement for federal departments and agencies to develop and implement telecommunications and automated information systems security education and training programs, as well as awareness activities.

Just issued in January was an advisory memorandum on office automation security guidelines. And the NTISSC currently has under various stages of development and review guidance pertaining to password security, labeling of media, accountability, audit trails, and risk analysis.

Sensitive, But Unclassified Information Protection

Perhaps no policy that we promulgated, however, was more misunderstood than the policy on sensitive information that was issued last fall by the Chairman of the Steering Group. A copy of this policy statement is attached for inclusion in the record.

Seriously misinformed critics erroneously claimed that this national policy on sensitive information protection gives the Department of Defense (DoD) the authority and "the right to restrict public access to not only classified information, but also to any civilian agency information which it considers unclassified, but sensitive." It categorically does not give

DoD, NSA, or any other agency any such authority. Let me clarify what the policy on sensitive information does and does not do.

The new policy does not give the Department of Defense or, importantly, the DoD's NSA the authority to restrict the dissemination of unclassified information. Simply put, the new national policy alerts all Federal Department and Agency heads to ensure that they take prudent steps to protect telecommunication and automated information systems used to store, process, or otherwise handle sensitive, but unclassified government or government-derived information. The definition of such information is "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens." This definition of sensitive information is essentially the same as the definition of sensitive information that is contained in H.R. 145. The essential thrust of the policy is to protect systems storing and processing such information against unauthorized access.

The policy simply reflects a recognition that technological advances have greatly increased the opportunity for unauthorized access to and, thus, abuse of sensitive, but unclassified information. And we believe it is essential for, and incumbent upon, the government to initiate measures to prevent the abuse or misuse of this information by those who would seek to invade the privacy of U.S. citizens, to obtain an unfair advantage in business dealings, to avoid law enforcement efforts, or to circumvent the intent and purpose of laws passed by the Congress. The policy is not intended to and will not affect authorized access to government or government-derived information. For example, the releasability of information to the media or individuals in response to a request submitted under the Freedom of Information Act is not affected by this policy.

The policy does not establish a new category of classified information. Indeed, the foreword to the policy states that the definition and requirements to safeguard classified information are addressed in Executive Order 12356, signed by President Reagan on April 2, 1982. Moreover, the policy does not specifically identify what sensitive, but unclassified information should be protected. Federal department and agency heads are individually responsible for identifying sensitive, but unclassified information, and for ensuring that telecommunication and automated information systems processing such information are appropriately protected against unauthorized access. It is the agency head who makes this determination--not DoD or NSA, or anyone else.

The policy was developed over a two-year period by subcommittees and working groups of the NTISSC. And, after the policy was developed and approved by the NTISSC, it was thoroughly coordinated and approved by the Systems Security Steering Group, the Cabinet-level body that is charged by the President with overseeing the implementation of NSDD 145. As I mentioned before, the Steering Group is chaired by the Assistant to the President for National Security Affairs, and composed of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Director of the Office of Management and Budget, the Attorney General, and the Director of Central Intelligence, all of whom are civilians.

Finally, let me assure you that the policy does not apply to information in the private sector. The intent of NSDD 145 and the policies that flow from it is to encourage, advise, and assist those in the private sector who want and need to protect their data, but only if that help is requested.

NSDD 145 recognizes that the protection of private sector information is not a matter that the government has the authority to unilaterally prescribe, but rather that it is an area in which the government should work in partnership with the private sector. In fact, NSDD 145 calls for the fostering of an "appropiate partnership" between government and the private sector. The tenor of the entire document is one of government cooperation with the private sector, not government direction of it. Accordingly, the document says "the government shall encourage, advise, and, where appropriate, assist [emphasis added] the private sector," and that "information and advice from the perspective of the private sector will be sought" with respect to implementation of NSDD 145 policy. The President's directive, therefore, represents recognition of the fact--at the highest levels of our government--that communications security and computer security are related disciplines, and that solutions to problems in those areas require a coordinated, comprehensive, approach that is national in scope.

H.R. 145, The Computer Security Act of 1987

I have submitted to your staff for consideration a draft of the original H.R. 145 in which I have personally made some suggested minor modifications. I believe that we can collectively work from this slightly modified draft to quickly reach an acceptable version of H.R. 145. Such legislation would provide for more robust and shared government-wide responsibilities in the information security area. In particular, there is a significant role defined for the Secretary of Commerce and the National Bureau of Standards working with the established National Computer Security Center and the Secretary of Defense as Executive Agent for all government communications and information security.

We would very much appreciate the opportunity to achieve closure on such legislation as it should further enhance information security across both the Federal and private sectors. Thank you very much for this opportunity to present my views on this vital area.

Table #1

SYSTEMS SECURITY STEERING GROUP

Chairman
The Honorable Frank C. Carlucci
Assistant to the President for National Security Affairs

Executive Secretary
Lieutenant General William E. Odom, USA
National Manager for Telecommunications and
Automated Information Systems Security

Members
The Honorable George P. Shultz
Secretary of State

The Honorable James A. Baker III
Secretary of the Treasury

The Honorable Caspar W. Weinberger
Secretary of Defense

The Honorable Edwin Meese, III
Attorney General

The Honorable James. C. Miller III
Director, Office of Management and Budget

Robert Gates
Acting Director of Central Intelligence

Table #2

National Telecommunications and Information Systems Security Committee (NTISSC)

Chairman
The Honorable Donald C. Latham
Assistant Secretary of Defense C^3I

Executive Secretary
John C. Wobensmith

Members

NSC
Department of State
Department of the Treasury
Department of Defense
Office of Management and Budget
Department of Justice
Department of Commerce
Department of Transportation
Department of Energy
Director of Central Intelligence
General Services Administration
Office of the Joint Chiefs of Staff
Department of the Army
Department of the Navy
Department of the Air Force
United States Marine Corps
National Security Agency
Defense Intelligence Agency
Federal Bureau of Investigation
Federal Emergency Management Agency
National Communications System

Observers

Federal Communications Commission
Intelligence Community Staff
Defense Communications Agency
National Aeronautics and Space Administration
Nuclear Regulatory Commission
Chairman, SAISS
Chairman, STS

Table #3

SUBCOMMITTEE ON TELECOMMUNICATIONS SECURITY (STS)

Chairman
William A. Bayse
Assistant Director, Technical Services Division
Federal Bureau of Investigation

Executive Secretary
Maureen Wise

Members
Same membership as the NTISSC

Observers

Federal Communications Commission
Defense Communications Agency
National Aeronautics and Space Administration
Drug Enforcement Administration
United States Customs Service
Intelligence Community Staff
Nuclear Regulatory Commission
United States Secret Service
Chairman, SAISS

Table #4

SUBCOMMITTEE ON AUTOMATED INFORMATION SYSTEMS SECURITY (SAISS)

Chairman
Patrick R. Gallagher, Jr.
Director, National Computer Security Center

Executive Secretary
Gerald L. Everett

Members
Same membership as the NTISSC

Observers
Department of Agriculture
Department of Education
Department of Health and Human Services
Department of the Interior
Department of Labor
Office of Personnel Management
Veterans Administration
National Aeronautics and Space Administration
Nuclear Regulatory Commission
Deputy Undersecretary of Defense (Policy)
Intelligence Community Staff
Federal Communications Commission
Defense Communications Agency
Chairman, STS

NTISSP No. 2
29 October 1986

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

NATIONAL POLICY

ON

PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SSSG
SYSTEMS
SECURITY
STEERING
GROUP

CHAIRMAN

FOREWORD

NSDD-145, "National Policy on Telecommunications and Automated Information Systems Security," signed by the President on 17 September 1984, in part provides policy and direction for systems protection and safeguards for telecommunications and automated information systems that process or communicate sensitive but unclassified information. The NSDD-145 Systems Security Steering Group has established that sensitive, but unclassified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however, the determination of what is sensitive, but unclassified information is a responsibility of Agency heads. Executive Order 12356 prescribes requirements for classifying, declassifying, and safeguarding national security information.

This policy and the principles and procedures contained in Office of Management and Budget (OMB) Circulars Nos. A-123 and A-130, "Management of Federal Information Resources," are complementary.

John M. Poindexter

NATIONAL POLICY
ON
PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information will protect such information to the level of risk and the magnitude of loss or harm that could result from disclosure, loss, misuse, alteration, or destruction.

SECTION II - DEFINITION

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information.

SECTION IV - RESPONSIBILITIES

This policy assigns to the heads of Federal Government Departments and Agencies the responsibility to determine what information is sensitive, but unclassified and to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems. The Director of Central Intelligence shall, in addition, be responsible for identifying sensitive, but unclassified information bearing on intelligence sources and methods and for establishing the system security handling procedures and the protection required for such information.

Federal Government Department and Agency heads shall:

a. Determine which of their department's or agency's information is sensitive, but unclassified and may warrant protection as sensitive during communications or processing via telecommunications or automated information systems. This determination should be based on the department's or agency's responsibilities, policies, and experience, and those requirements imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted;

b. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information requiring protection;

c. Determine, in coordination with the National Manager, as appropriate, the threat to and the vulnerability of those identified systems and;

d. Develop, fund and implement telecommunications and automated information security to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

e. Ensure implementation of telecommunications and automated information systems security consistent with the procedures and safeguards set forth in OMB Circular A-123 and A-130.

The National Manager shall, when requested, assist Federal Government Departments and Agencies to assess the threat to and vulnerability of targeted systems, to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.

Mr. McCurdy. The next witness is Lieutenant General Bill Odom.

Welcome. It's good to see you again. Thank you for coming to testify today and your full statement will be admitted into the record in its entirety, and we look forward to your comments.

General, pull your microphone and turn the switch there.

STATEMENT OF LT. GEN. WILLIAM E. ODOM, DIRECTOR, NATIONAL SECURITY AGENCY

General Odom. Is that on now?

Mr. McCurdy. They aren't sensitive microphones, you're not used to them, those in your business we understand, but we need them in this room. Thank you——

General Odom. Mr. Chairman, thank you very much for the opportunity to submit a statement. I will not elaborate on it, but rather offer just short remarks in response to some of the things that I've heard here this morning in answer to your questions.

I could not agree more with Mr. Glickman on the necessity to protect our rights, to be sure that the access to information is not impeded. I cannot underscore enough what Mr. Latham said, Secretary Latham said, about who has the authority to lock up what kinds of information.

I do not see it as my role, and I have no direction telling me to tell anybody else what they must put in a locked up computer or a safe, a room, or any other sort of security device.

The other thing I would like to agree with you on is the definition of the problem, which I gather enlightened a number of people in the hearing last year with testimony showing the complexity of this computer security problem and why it's not an easy thing to make them secure. In fact, it's very difficult. In the task that we have received, under Mr. Latham's interagency committee and the steering group, is to look into that problem because we just happen to have a lot of people who are fairly competent in computer matters, to take that intellectual expertise, and to try to define the problem and get some solutions to it.

It was my experience before I came to NSA, when I was in the Army as the Assistant Chief of Staff for intelligence and concerned with security, when I was asked by various organizations within the Army where can they buy secure computers, such computers weren't available. The problem today, as we see it, is to do research that will support vendors in the private sector learning how to make them secure. And people, buyers, can choose to do with them what they're authorized to do, or what they have the discretion to do; that's totally out of my area of responsibility, concern, or basic worry.

I would like to invite all of you, if you have the chance, to come out and see the National Computer Security Center and talk to the people there, because I think it will give you a much better sense of what it's about and what it's not about.

As far as the research effort, consultative effort, I'll give you an example of the kind of thing that it can do, and we've had a little success in. I'm very modest about what success we've had so far. A department of this government, a civilian department, had about a

$400 million contract for some automation that they were going to purchase. The vendor said that certain security levels couldn't be met. They belatedly, after they were already beginning to work on this contract, asked us to come and look at it.

Some of our consultants reviewed it, gave them advice, technical advice on how to confer with their contractor. It turned out that the contractor, when they specified things certain ways, could meet those security standards, and therefore, a considerably higher level of security will be available on that ADP in two of our civil departments in the government.

Those are the major points I want to make. One other last remark I should perhaps add; the task is very large. We already are coordinating with the National Bureau of Standards and have shared part of the work with them. We have an outreach program to universities that we are trying to get started; it's not formal yet, but it's clear to us that universities must play a role in research. We certainly can't afford to do all the research. We just don't have the people. We don't have the money, and I don't think you would ever appropriate the money for us to build the empire that would be required to do all the research.

I must say I'm a little puzzled at the allegation that we would invade people's privacy or block the flow of information. Our interaction with university faculties has not brought the same kind of criticism. They seem to be comfortable with our approach.

If I ask myself what the explanation is, I think it may be that they've been in the computer center, seen what it's about, and therefore see such fears are groundless. I am willing to do anything that you would desire to move what seems to me to be a fundamental misimpression that we somehow are a threat to privacy.

I would also say you have committees in both Houses of the Congress who oversee our agency, and you certainly have very strong mechanisms for investigating any suspicions you might have that we were transcending what's an appropriate role in that regard.

Thank you, sir.

Mr. McCURDY. Thank you, General Odom.

As you know, as reported earlier, there have been some press accounts about agents, various intelligence agencies, whether it was the CIA, or NASA, Air Force, or FBI visiting certain data base service providers, asking them to disclose their customer lists.

Can you comment on these allegations, and if true, what would be the legal authority for such a request?

General ODOM. I'm not familiar with the particular cases you have. I can certainly ask my staff and get an answer to it. I suspect that it came up in a matter of consultations with them about how they could secure a system. If you don't—if someone asks, "How do I secure my internetted system here?" If you don't know all the entry points into it, it's difficult to know where to put blocks or checks against unwanted access.

Now, that would be my guess about what happened; that's what I would expect to discover if I went to that department and asked them about it.

Mr. McCURDY. I would appreciate if you would provide for the record the response to that by your staff.

Concerning the data encryption standard used for protecting unclassified communications in the government and in private sector, why did the NAS announce it would not certify DES products after 1988, and what would have replaced it?

General ODOM. The encryption capability has a life which is determined to some degree by the ability of people who want to break that encryption device: what they learn about it and the computing power and other factors they can bring to bear against it.

If you take a single encryption system and put it out there, it's secure for a while. As people learn more about it, it eventually tends to be broken. Therefore, any DES or CCEP will have a limit beyond which one could not say, with a high degree of confidence, will be secure.

What we essentially said is that uncertainties would appear to us to be on the horizon for DES thereafter.

Mr. McCURDY. And how do you address those uncertainties in the future?

General ODOM. Well, we design new standards, new devices.

Mr. McCURDY. Would you accept a compromise arrangement that gave a civil agency such as NBS the final authority for establishing computer security standards for protecting unclassified information, and responsibility for interacting with the private sector which made full use of NSA's expertise?

General ODOM. The general thrust and spirit of what you say, sir, sounds highly acceptable. The details of what that would mean with regard to who's doing what part might be less attractive to us than others. I would have to examine that in more detail.

That is the major concern I would have, and I am, in this regard, merely following the Administration's position. I didn't create NSDD-145. I found myself in charge of an agency with the task already in hand to execute.

I must say after I had reviewed it, though, I see that it makes considerable good sense with regard to conservation of resources and the lack of duplication in government funding.

If that kind of compromise did not lead to starting all over and building duplicate activities, then I think we would be supportive of it. We are already trying to find pieces of the task that appropriately reside in NBS. I think there's a fairly symbiotic division of labor that withhin the past year in particular that has emerged between NBS and the National Computer Center.

Your own General Accounting Office rendered a report that judged the technical competence at the National Computer Center to be fairly advanced compared to NBS. Transferring some parts of the task there would be backing up and starting over. Others quite clearly can be transferred.

So, in spirit, I definitely accept it. I think one would have to get down to the details to know what compromise makes sense.

Mr. McCURDY. But you know the other two hats I wear is as a member of the Armed Services Committee and also the Intelligence Committee, and I would suggest that there is a very small window of opportunity here for achieving a compromise. And that if a compromise is not worked out, then, I think there's a fairly good chance that the gentleman from Texas, Mr. Brooks, will have a bill that does not have the input that you would like to provide.

So, I think that it is important that we take that step and I appreciate your willingness to do so. And with that I'd like to recognize the gentleman from Pennsylvania, Mr. Walgren, who is Chairman of the SRT Subcommittee that we are——

General ODOM. Mr. Chairman, let me add that what Secretary Latham said, I follow his general guidance on that matter with regard to dealing with the committees in legislation.

Mr. MCCURDY. Very good. I think we're making some progress. Mr. Walgren.

Mr. WALGREN. Well, thank you, Mr. Chairman.

And perhaps I could ask that an opening statement that I had be made part of the record at the appropriate place.

Mr. MCCURDY. Certainly, without objection.

[The prepared opening statement of Mr. Walgren follows:]

OPENING REMARKS
OF
THE HONORABLE DOUG WALGREN
FOR
HEARING ON H.R. 145, THE COMPUTER SECURITY ACT OF 1987

February 26, 1987

Every day it seems, we read new revelations about the inside stock trading scandal in New York. While this scandal is shocking, it pales in significance to another scandal which is going on today right here in Washington, in Baltimore, and in a number of other cities around the country. While the Wall Street thieves steal their millions, the Federal computer thieves have been stealing their billions. In 1985 testimony before this Committee the Inspector General of the Department of Health & Human Services estimated that at least a billion dollars had been stolen from his agency alone.

The Federal scandal, like the Wall Street scandal, is an inside job. Dozens of caseworkers, clerical employees, data entry technicians, and supervisors have been convicted of diverting money from benefit or payroll systems to their own use. These individuals change the address of deceased or ineligible benefit recipients, or create false claims and arrange for the resulting benefit checks to be mailed to co-conspirators. The average loss to the government has been at least 100 thousand dollars by the time a thief has been discovered.

Experts are convinced that the convictions to date represent only the tip of the iceberg. Those who have been caught usually have been

UNLUCKY ENOUGH TO MAKE A MISTAKE THAT HAS BEEN DISCOVERED BY A CO-WORKER. THE GOVERNMENT'S WEAK SYSTEMS FOR DISCOVERING COMPUTER FRAUD ALMOST NEVER UNCOVER A THIEF BY THEMSELVES.

BOTH TECHNICAL AND ADMINISTRATIVE ASPECTS OF FEDERAL COMPUTER SECURITY ARE INCREDIBLY WEAK. THE GENERAL ACCOUNTING OFFICE IN 1985 TESTIFIED IN GREAT DETAIL ABOUT THE LACK OF AUDIT TRAILS AND THE FAILURE TO HAVE EVEN THE MOST RUDIMENTARY OF SAFEGUARDS IN CERTAIN SYSTEMS WHICH DISPENSE MILLIONS IN BENEFITS . WE LEARNED OF INSTANCES WHERE SUPERVISORS HAVE NO UNDERSTANDING OF THE COMPUTER SYSTEMS USED BY THEIR EMPLOYEES. WE HEARD OF EMPLOYEES WITH CRIMINAL RECORDS BEING ASSIGNED TO RUN PAYROLL SYSTEMS. WE HEARD OF PASSWORDS TAPED TO COMPUTERS AND SENSITIVE SYSTEMS BEING LEFT RUNNING AND UNATTENDED.

FORTUNATELY OUR FEDERAL COMPUTER SECURITY PROBLEMS ARE SURRMOUNTABLE IF PROPER PROCEDURES ARE PUT IN PLACE AND EMPLOYEES ARE GIVEN APPROPRIATE TRAINING. THE NATIONAL BUREAU OF STANDARDS THROUGH ITS INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY (ICST) HAS ALREADY PERFORMED MUCH OF THE RESEARCH AND DEVELOPED MANY OF THE STANDARDS WHICH ARE NEEDED. THE BILL BEFORE US WOULD GIVE THE BUREAU THE AUTHORITY TO ISSUE STANDARDS AND GUIDELINES TO PROTECT THIS SENSITIVE CIVILIAN INFORMATION. THE ICST AT THE BUREAU HAS A LONG HISTORY OF WORKING WITH OTHER GOVERNMENT AGENCIES AS WELL AS THE BANKING AND COMPUTER INDUSTRIES. IN MY VIEW ICST IS THE IDEAL ORGANIZATION TO DO THIS NEEDED WORK.

IN CONTRAST, THE ADMINSTRATION IS PROMOTING A CURE FOR OUR COMPUTER

SECURITY PROBLEM THAT IN SOME WAYS MAY BE WORSE THAN THE DISEASE. IT HAS PUBLISHED NATIONAL SECURITY DECISION DIRECTIVE - 145 WHICH PUTS THE NATIONAL SECURITY AGENCY OF THE DEFENSE DEPARTMENT IN CHARGE OF COMPUTER SECURITY GOVERNMENT WIDE. I AM CERTAIN THAT THE PROPRIETY OF PLACING A TOP SECRET AGENCY OF THE DEFENSE DEPARTMENT IN CONTROL OF THE SECURITY OF THE COMPUTERS WHICH AFFECT SO MANY ASPECTS OF THE LIVES OF PRIVATE CITIZENS WILL BE EXPLORED IN GREAT DETAIL IN THESE HEARINGS.

IN CLOSING, I WOULD LIKE TO COMPLEMENT CONGRESSMAN GLICKMAN ON HIS UNTIRING EFFORTS TO BRING THIS IMPORTANT PROBLEM TO A LEGISLATIVE SOLUTION. I HOPE WE WILL BE ABLE TO BRING THIS LEGISLATION FORWARD QUICKLY SO THAT REFORMS CAN BEGIN AND COMPUTER THEFT FROM THE GOVERNMENT CAN BE REDUCED TO A BARE MINIMUM.

Mr. WALGREN. And at this point I would only say that on behalf of our subcommittee that we certainly attach a tremendous amount of importance to this area, and are very pleased to see your subcommittee moving with it. And we're following it with interest. We do think that there's an opportunity to do something here that would be very constructive and that maybe some of the alternatives down the road are not that good.

So, we want to join with you in looking for that compromise, and we'll work with you to that effect.

Mr. MCCURDY. Thank you, Mr. Walgren.

The gentleman from Kansas, Mr. Glickman.

Mr. GLICKMAN. Thank you, Mr. Chairman.

General, first I want to take you up on the offer to go visit the Center. I've never been out there. I've passed by it on Amtrak——

General ODOM. That's too quick a view.

Mr. GLICKMAN. Pardon?

General ODOM. That's too short a view. I advise you to spend more time.

Mr. GLICKMAN. So, we ought to get out there. Let me ask you, while I agree that you have a relationship with the National Bureau of Standard, and the co-sponsor of this conference, again, my concern relates to the substantive problem which exists, which was identified specifically by the Inspector General of HHS who said quite clearly that there is an enormous amount of work to be done at the federal agencies to protect the information contained in federal computers, all the way from individual records to systems of our society. So far there hasn't been a very good job done in this area. And therefore, it's still my feeling that, particularly in civilian agencies, civilian information, that some of it may be sensitive.

But notwithstanding the good work that you're doing, it's not getting implemented into the nuts and bolts of the operation of those agencies, and that was identified by HHS. And that's why this bill came along to provide a mechanism for mandatory training, for example, you know, of government workers, computer security training.

We felt very, very concerned about giving NSA that particular responsibility. And it shouldn't have that responsibility. You're more of a research type Center and you set standards. And, you know, all the stuff you've done on encryption and everything else.

So, I want to make it clear that this issue has become a turf fight as much as anything over the years. It's not related to the substantive problem. The problems are real, they need to be solved. If we can work these things out, and basically protect everybody's turf, actually, if we protect everybody's turf we probably haven't done anything. But if we can work it out and do what needs to be done to protect that civilian information, and those kinds of computers, I think we've done the world a service.

That's why I'm glad to see you and Mr. Latham and the National Bureau of Standards say, okay, maybe we've got something that we can work out.

And, you know, I understand where you said you were a little puzzled about everybody's concerns, about the restriction of the flow of information. But I think largely that goes to the fact that we are concerned about certain things that have happened within the National Security Council and other related areas that don't really have anything to do with your operations in Baltimore. And so, I think that needs to be stated.

Now, do you train—do you have any formal training programs with other federal agencies right now on computer security?

General ODOM. Not that I know of.

Mr. GLICKMAN. What's your non-classified—do you have a classified?

General ODOM. A classified and an unclassified.

Mr. GLICKMAN. And the unclassified is with what, specific agencies or——

General ODOM. Mr. Latham wants to send somebody else up to answer.

Mr. GLICKMAN. I mean, do you have—is there some sort of formal training program that you have?

General ODOM. Why don't you elaborate on that.

Mr. GLICKMAN. Does somebody want to tell us what you actually do right now?

Mr. McCURDY. Just identify yourself for the record, please. I don't think he heard that. Use the microphone.

Mr. GALLAGHER. My name is Pat Gallagher and I'm the Director of the National Computer Security Center.

We have a set—a number of formal training programs. We have one that covers classified things and that's to be done in that context. We have one which is not classified, and is for anyone in the government who wishes to partake in that.

We find ourselves at most of the conferences and conventions that are germane around the United States that are either dealing with data processing or computer security, either giving speeches or presentations or modules in their kinds of things.

We have, of course, an enormous amount of literature that we have created, some of it is technical as in our orange book which sets criteria; some of it which is more, let's say, general which talks about procedures and what one should do in the environment to protect computers, because the problem is both a technical problem and a managerial problem. And we mail out that literature to anyone who has a legitimate—who makes a legitimate request for it.

It goes then—the spectrum on down to things even like just handouts at conferences, and posters, and those kinds of things.

In addition to that, we are launching an effort at universities to see if we can both stimulate research and have courses taught in the computer security or better said, in computer discipline. Because really what we're talking about in much of this business is the way—is a discipline design of machines, and the discipline writing of software. And so that then is a technical—it's a technical art, a technical talent which is very germane to an academic institution.

And we're in the process—we've started a process with the University of Maryland, for example, who has a strong Computer Science Department, to begin to nuture courses and research; some of which then could be transmitted through Maryland's television networks, academic television networks, to allow us to reach out and touch American universities, American academ, government and civil sectors.

So, I think, though, and not totally complete, and though we're not absolutely satisfied yet, there is a broad spectrum of reaching out and touching in an academic training on that.

Mr. GLICKMAN. Do you feel in any way that you are competitive with the National Bureau of Standards, what they are currently doing in this area?

Mr. GALLAGHER. I don't think so. I've been working very hard at being very complimentarily with Mr. Burrows and his operation. He and I meet every two months to talk about what it is that we're doing, we at the Center, and what it is that he's doing at the Institute.

We have transferred funds to him recently to do some efforts in the areas of protocols which we think are extraordinarily important. We are beginning to talk about how we will share with them some of the work in evaluating what we call components, subassemblies of computers and data processing things, that perhaps they are better and stronger at doing than we are. And so, therefore, we should maximize their talents for what they do well and our talents for what we do well.

I do not perceive a destructive competition. We may be intellectually competing with one another, but that's probably stimulating.

Mr. GLICKMAN. Well, thank you, General Odom, for your testimony. And I think that this testimony points out the fact that we can devise a way of doing this that in fact is not destructive, is not duplicative. It does what I think our goal is, and that is to ensure that these federal agencies have a high priority to do their job of protecting that data base which they have not done. And both the NBS and NSA can have relative respective roles.

I just may give you one anecdotal bit of information. When we had our hearings here before, I believe Tony—we had somebody from Los Alamos who testified they were broken in to, and the password that was utilized at Los Alamos Laboratory was Joshua, which was the same password used in the movie "Wargames." And in fact, the password had not been changed six months before or several months after the movie came out.

It was an example of just totally—whether it's non-caring or the agency had no concept of what it was in protecting that information. And we just want to make sure that doesn't happen.

Mr. McCURDY. I thank the gentleman. Of course, having a son named Joshua I can understand the popularity of the word.

Being Subcommittee Chairman has some prerogatives, and one of those is that I wanted to recognize two gentlemen in the back of the room that are State Representative and State Senator from my District in Oklahoma, Senator Paul Taliaferro and Representative Sid Hudson. And we're certainly glad to have you all in Washington. I didn't know you were going to be here.

General Odom—let's see, the gentleman from Missouri, Mr. Buechner, do you have any questions?

Mr. BUECHNER. Yes. You see, I had my questions in advance, so I didn't have to be here.

Does NBS have any difficulties or problems with coordinating computer security activities with NSA?

General ODOM. I think you've just heard the comments by Mr. Gallagher, and I would reaffirm those. I'm sure there has been some intellectual competition. I think now, at least in the last six months to a year, the division of labor is beginning to become clear, and a fairly complementary interaction is taking place.

Mr. BUECHNER. How does this bill—have you reviewed the bill, H.R. 145, and how would it impact the relationship, as you see it?

General ODOM. Well, my general impression is that it would give NBS responsibility for a lot of things that we are doing now and would essentially build a duplication, presumably for two different sectors. In other words, NBS would be building computers that are secure for civilian agencies, non-intelligence or military activities, and NCSC would be securing computers or developing a program for those in the Defense Department.

Now if the technology, the technique, and the know-how for computer security were different in those two areas, I could see strong logic for that division. But thus far, it appears that it isn't different. It appears that all of us have a high level of ignorance about it and that we need to use our resources as efficiently as possible to meet the urgencies that Mr. Glickman pointed out.

Therefore, my concern with the bill is not so much some of the issues that have been raised as resources against the problem in general and how it can be done efficiently. Any part of that bill which seems to me to be efficient in that regard, I'm absolutely supportive of.

I personally don't have problems with the bill, except in terms of available resources. I have found that it's kind of a thankless job when you try to get people to contribute money to this effort; it's very hard to come by.

One of our worries about duplication is that it will be more difficult to get money to support this problem. That is the major factor that concerns us. It's not these other kinds of matters. Everybody wants it, but nobody wants to pay for it.

A lot of the federal agencies want security, but they don't want to put up the money for it. That's understandable when some of their other priorities get more public attention or more operational attention.

Mr. WALGREN. Would the gentleman yield?

Mr. BUECHNER. Certainly.

Mr. WALGREN. Just on the thought of the propriety, though, of our using military dollars for a function that is something that these other agencies should be doing for themselves, and yet they are not attracting the dollars for whatever reasons, perhaps our own shortcomings in appreciating the services that they are providing for the public.

It may be not helpful for us to throw the military into that breach.

General ODOM. I think you heard the Secretary here say earlier that a national funding mechanism to get everybody to pay his way in that regard is highly desirable. To the extent that the bill does that, I'll tell you, the Defense Department would be very supportive.

I am accused by people in the Defense Department of being a sumphole for money to go do other agencies' activities. I have a very unpleasant position to occupy in all of this. I've experienced a lot of cross-pressures in this regard.

Mr. WALGREN. I thank the gentleman for yielding.

Mr. BUECHNER. Do you have any cost estimates of losses that have been incurred by either federal or civilian, due to breaches of computer security?

General ODOM. I don't have any at hand. We could do some research out in the Computer Center and see if that's available.

Mr. MCCURDY. We may have some witnesses later that may.

General ODOM. We could try to find some material on that for you, sir, and submit that for the record.

Mr. BUECHNER. Yes. I think it would be important for us to be able to ascertain the magnitude of the problem. Obviously the response is always—or should be—in direct relationship to the problem. And so if you could provide those for the record, I'd certainly appreciate it.

Thank you, Mr. Chairman.

Mr. MCCURDY. I thank the gentleman from Missouri.

The gentleman from North Carolina.

Mr. PRICE. Thank you, Mr. Chairman.

General Odom, just to follow up a little further on the matter of interagency coordination, you refer in your statement to an interagency agreement with the FAA.

I wonder if you could elaborate a bit on that agreement? First of all, what is the computer security issue here? What is at stake, and exactly how has that agreement worked? When was it concluded, under what authority, and so forth?

General ODOM. I'm going to ask Mr. Gallagher to answer that question.

[General Odom and Mr. Gallagher confer.]

General ODOM. I'll have to answer for the record on that. I don't have the details to give you a proper answer to that right now.

Mr. PRICE. Well, I think that kind of description would be helpful.

Was that agreement completed before or after the Poindexter Memorandum?

General ODOM. I would be surprised if it were before, but I could be wrong.

It was before? If it happened before, then it was probably as a result of their initiative, coming to us and asking for help.

Mr. PRICE. Well, it would be helpful to have the details on that and to also have you explain in what way, if any, the Poindexter Memorandum would have altered the terms of such interagency agreements or made them more feasible.

General ODOM. If there's something wrong with our system, we'll change it. The object of the whole process is to make this kind of technology and know-how and advice easier to get to for all agencies of the Government. And if it has turned out to work the other way, then we're going to have to repair it.

Mr. PRICE. Well, I wouldn't assume that it's worked the other way, but it is of interest, I think, that this kind of agreement was concluded earlier, and it would be of interest to know in what ways it has proved satisfactory and in what ways it has not so.

General ODOM. We will get you a proper answer to that.

Mr. PRICE. Thank you, Mr. Chairman.

Mr. McCurdy. I thank the gentleman.

The gentleman from Maryland.

Mr. McMillen. General, welcome. I am looking forward to visiting your Computer Center with our chairman in a week or so.

One of the things I hope to achieve in visiting there is to understand a little bit of the jurisdictional lines that are drawn here. As I was reviewing this legislation, I seemed to get a sense of what the National Bureau of Standards' mandate is in this regard in maintaining the security standards and so forth, but I'm not exactly sure as to your mandate in going forward.

I think it has occurred to most of the committee that this is not confrontational. You've had a cooperative working relationship.

Maybe you could outline for me just a little bit how you work together? It seems to me that you're offering technical and consultative services and so forth. How do you work with the Bureau on those?

General Odom. Well, there are a couple—at least one conference sponsored each year on it. And Mr. Gallagher, the head of the Center, has a lot of direct and personal relations with the NBS in the general. The NTISSC arena brings NBS into direct relationship with our National Computer Security Center. Those are the major fora right now.

That's a fairly dynamic and changing matter, because as we learn that the nature of the problem is X or Y, we begin to develop new ways to interact and new ways to allocate what's to be done.

As I mentioned here earlier, I think the level of ignorance about how to do this is fairly high, and as we make progress, some of the initial misunderstandings and quarrels, I think, subside a bit, and indeed, we do discover there's a lot of work for everybody.

Mr. McMillen. In the Business Week article, it says, "The Pentagon believes the Soviets are so adept at harvesting data bases that they are closing the technological gap faster than ever before."

Do you think the DOD has done an adequate job of protecting——

General Odom. It hasn't been possible to give what I would consider adequate protection, because the technology for security in the computer area is non-existent.

We have published the Orange Book standards, and when you come out, we will show you a chart matrix with some computer products we're prepared to say meets those standards. A year ago, we only had one or two of cells in the matrix with something in it. The number has increased in the past year, so that the prospects of buying capabilities to meet those standards is slowly growing. But I would describe them today as wholly inadequate.

Mr. McMillen. I didn't get a chance to ask this, but what is your opinion on the establishment of a Privacy Advisory Board within the Commerce Department?

In this legislation, there is established a Computer Systems Security and Privacy Advisory Board. Are you familiar with this?

General Odom. I'm not familiar with the details of the advisory board. In principle, I don't know why it would be a problem for us. But as I mentioned earlier, the major concern of mine is not an advisory board or some detail like that. It's the fragmentation of resources to throw at the problem.

Mr. McMillen. Thank you very much.

Mr. McCurdy. I thank the gentleman.

General, I want to thank you very much for appearing today. We look forward to working with you in the near future on trying to resolve this issue and look forward to seeing you next week also.

General Odom. Thank you very much, Mr. Chairman.

Mr. McCurdy. Yes, sir. Thank you.

[The prepared statement of General Odom plus questions and answers follow:]

STATEMENT BY

LIEUTENANT GENERAL WILLIAM E. ODOM, USA

DIRECTOR

NATIONAL SECURITY AGENCY

AND

NATIONAL MANAGER

NATIONAL TELECOMMUNICATIONS AND AUTOMATED INFORMATION

SYSTEMS SECURITY

CONCERNING H.R. 145

BEFORE THE

SUBCOMMITTEE ON

TRANSPORTATION, AVIATION, AND MATERIALS

AND THE

SUBCOMMITTEE ON

SCIENCE, RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

FEBRUARY 26, 1987

Mr. Chairman and members of the subcommittees:

Thank you for the opportunity to appear before you and to present my views on H.R. 145, the Computer Security Act of 1987. I am of the view that the attention being paid to computer security by your subcommittees, the full Science, Space, and Technology Committee, and the House Committee on Government Operations have done a great deal to raise the awareness of not just Federal employees, but the American public at large, that computer security is a national problem. I thank you for that help in raising everyone's consciousness, and hope we can work together to find solutions to the problem.

I am concerned, however, that the proposed legislation at hand, as it is currently drafted, does not lend itself to a unified, government-wide, national approach to the issues of computer security. I see in the legislation many similarities between it and the version of H.R. 2889 that the Committee on Science and Technology reported to the House floor in August of last year. And in reviewing the report that accompanied H.R. 2889 I see that, notwithstanding the extensive hearings that were held on that bill, there remain some fundamental misunderstandings about what NSDD 145 accomplishes, and NSA's role in the NSDD 145 process.

The report claims that,"[a]lthough NSA has a fine track record as the lead technical agency for securing ADP systems containing national security data, it is not clear that it is the appropriate lead agency for directing civil agency computer security." The report points out that "NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies," and calls for "a civilian authority . . . to develop standards relating to sensitive, but unclassified data." The report alleges that the composition of the interagency committee created by NSDD-145, the National Telecommunications and Information Systems Security Committee (NTISSC) "favors military and intelligence agencies." The report points up a need for "greater emphasis [to] be given to cooperation between the military and civil agencies as well as the private sector in setting computer security and training goals," and states that this can be accomplished by "fostering greater communication and cooperation between the NBS and NSA in setting overall Federal computer [sic] policy."

First of all, let me say that the communication and cooperation that already exists between the National Security Agency and the National Bureau of Standards could serve as a model for the rest of our government. It is a well-traveled two-way street between Fort Meade and Gaithersburg. We are currently negotiating a formal, detailed Memorandum of Agreement that reflects and enhances our current, ongoing cooperative relationship in the field of Information Security. The agreement that we are negotiating outlines the responsibilities of and interrelationship between the National Bureau of Standards and the National Security Agency in implementing the requirements of NSDD 145 to secure automated information systems processing classified or sensitive, but unclassified, government or government-derived information; to protect federal government operated automated information systems processing information which is neither classified nor sensitive within the meaning of NSDD 145; and to assist the private sector in protecting its automated information systems processing information the private sector may choose to protect.

Our fine relationship with the National Bureau of Standards in the field of computer security, in fact predates NSDD 145 by a good many years, and we have worked together over the years to solve technical issues of common concern.

This fall, for example, we will be co-sponsoring with the National Bureau of Standards for the tenth time, our joint annual National Computer Security Conference. This conference is clearly the standard by which other computer security conferences are judged, with attendees from private industry and governments around the world. In fact, the conference is so successful that it has outgrown the facilities at Gaithersburg, where it was held up until last year, and this year it will be held at the Baltimore Convention Center. Incidentally, Mr. Chairman, I would like to take this opportunity to personally invite you and your colleagues to attend this year's conference so you can see for yourselves, firsthand, the fine cooperation and communication that currently exists between the NSA and the NBS.

NSA and NBS are also currently very heavily involved in planning and executing computer security research and development; planning and conducting computer security training and awareness activities; participating in network security methodology and evaluation criteria development; and developing risk analysis methodology.

And Mr. Chairman, our cooperation with the National Bureau of Standards is by no means bilateral. NBS and the Director of the Bureau's Institute for Computer Science and Technology have, virtually since the inception of the NTISSC, and its Subcommittee on Automated Information Security (SAISS), played a key role on those bodies. The Director of the ICST has served, almost from the time the SAISS was created, as the Chairman of the SAISS Working Group that is responsible for publishing NTISSC standards, criteria, and guidelines.

The National Computer Security Center, established at the National Security Agency shortly after the President expanded the scope of its mission from its previous role as the DoD Computer Security Center when he signed NSDD 145, has made giant strides and a tremendous effort to meet the needs of the civil sector component of its expanded constituency.

As part of this effort, during August 1985, letters were sent to the heads of 79 organizations throughout the Federal government, including independent government establishments and government corporations, offering computer security assistance, outlining the services offered by the Center, and requesting a point of contact for computer security matters. A team from the National Computer Security Center visited these organizations between August 1985 and July 1986 to introduce them to the Center's mission, to discuss the need to protect sensitive data, and to make them more aware of the security measures available to protect sensitive data. The response from those agencies was very enthusiastic.

A separate branch has been established within the National Computer Security Center to support the civil sector of the government. The branch provides the following services:

Computer Security Enhancement Reviews - These programs consist of short-term (two days to one week) on-site technical analyses. They identify threats and vulnerabilities, provide an outbrief report of these vulnerabilities, and recommend methods to reduce the vulnerabilities. Computer Security Enhancement Reviews are in progress or have been completed at 11 civil departments and agencies.

Technical Consultations - These consultations provide a variety of support services, from discussions on a particular area of customer concern, to a one-time review visit. The one-time review visit is not as detailed as a Computer Security Enhancement Review visit, nor does it provide as much detail. It provides a very short review of the vulnerability of a system. Technical consultations are in progress or have been completed at 21 civil departments and agencies.

Request for Proposal (RFP) Security Review for Trusted Systems - This security review consists of assisting the customer with incorporating security requirements in the procurement process. Such security reviews are in progress or have been completed at eight civil agencies.

Security Policy Review - This takes the form of providing consulting assistance to customers during the drafting of computer security policy. A security policy review is in progress or has been completed at 14 civil departments and agencies.

In addition, beginning in May 1986, the Center embarked on a program, at the behest of the SAISS, aimed at familiarizing the civil sector with the applicability of the Center's Trusted Computer System Evaluation Criteria. I had issued the Criteria, in my role as National Manager, as a National Telecommunications and Information System Security Advisory Memorandum. Over forty civil departments and agencies took advantage of the training, and the Center is using information gained from those civil agencies during the course of the training to revise and update the Criteria, thus making it more applicable to the computer environments of those civil departments and agencies. When that job is finished, the NTISSC plans to issue the Criteria as an NTISS Instruction.

The National Computer Security Center has also published numerous computer security guidelines, standards, informational brochures, posters, leaflets, and videotapes. These have been distributed variously throughout the civil sector of government, private firms, and the academic community. Nearly 1100 copies of the videotapes alone have been distributed in a year and a half. I have brought copies of these publications with me for inclusion in the record of these hearings, and am providing you with copies of the videotapes so you may view them.

Are our efforts showing results? We believe that indeed they are. Let me provide three brief examples. They demonstrate how the National Computer Security Center has been assisting the Department of State, the Department of the Treasury, and the Federal Aviation Administration with developing Requests for Proposal (RFPs) to industry for trusted computer systems worth several billion dollars over the life of the contracts.

Last fall, the State Department released their RFP entitled "ADP Equipment and Services," with an estimated value greater than $400 million over a contract life of five years. After the RFP was released, the State Department was challenged by some vendors on the security requirements of the proposal that specified a "B2" level of trust. Basically, the vendors were claiming that a "B2" system would not be technically achievable in the time specified. The National Computer Security Center held a number of discussions with State Department officials. The talks included reviews and detailed discussions on the very sensitive information processed on State Department systems, the extremely hostile environment at some U.S. embassies, and the technical rationale behind specifying a "B2" level of trust for the systems in question. The Center also briefed the State Department on the status of vendors who are developing trusted products that would meet the Department's requirements. The State Department subsequently made the decision to leave the RFP as written. The National Computer Security Center will assist State in the technical review of proposals received from industry.

Moreover, the Treasury Department has released an RFP on the Treasury Minicomputer Acquisition Contract (TMAC) for comment. Treasury is planning to formally release the RFP in March or April. The TMAC will span a five-year period for the purchase of minicomputers throughout the Department, with the Internal Revenue Service being the primary beneficiary. The contract is estimated to be valued in excess of $600 million. Following the strategy of the draft policy in the NTISSC that is proposing the requirement for Controlled Access Protection (CAP), Treasury took the initiative to specify the CAP or "C2" level of trust as a minimum security specification. As a highly desirable feature that will receive additional credit, the "B2" level of trust was also specified. The National Computer Security Center drafted the security specifications for the RFP, and will be supporting Treasury in the technical review of the responses received from industry.

Under an interagency agreement with the Federal Aviation Administration, the National Computer Security Center has committed resources to provide a year-long effort to improve the computer security posture throughout the FAA. This included a study of the current Air Traffic Control System, a study of the interim host system, and an evaluation of the design specifications for the planned $11 billion Advanced Automation System. Work on this last system resulted in significant input to the developing RFP, the initial security policy for the system, and most significantly, setting the level of trust at the C2 level for hardware and software associated with the Advanced Automation System--steps that we believe will positively affect the safety of millions of future air travelers.

A little over a year ago, the National Computer Security Center moved into a facility close to Baltimore-Washington International Airport. We are making every effort there to make our laboratories and facilities state-of-the-art and second to none--as befits a national center of excellence. I should like to extend an open invitation for you to visit the Center and see firsthand for yourselves what we are doing. We currently have slightly over 300 people on board at the Center, and are actively recruiting to meet an authorized strength of nearly 350 people.

We at NSA have clearly made a significant investment in information security, and believe we have been responsible stewards of the funds you in the Congress have allocated, authorized, and appropriated to us over the years for information security purposes and for the good of the nation. I would hope that my testimony today helps to persuade you that the criticisms of NSA and the NSDD 145 structure that appeared in the report of the Committee on Science and Technology which accompanied H.R. 2889 were unfair and not justified.

We believe that, in a very short period of time, we have ably demonstrated that we can, indeed, serve the civil sector of our government just as well as we have our more traditional customers. We at the National Security Agency take pride in our role as a truly national agency, and look forward to further opportunities to expand our "fine track record as the lead technical agency for securing ADP systems," as your committee report so generously describes.

Thank you again for the opportunity to testify before you. That concludes my prepared statement. I would be happy to answer any questions you may have.

QUESTION: What is the nature of NSA's computer security effort with the FAA? Did the Poindexter Memorandum predate that effort or have any effect on it?

ANSWER: The FAA requested support from the National Computer Security Center at NSA in November 1985. A copy of that request is attached. Subsequent meetings resulted in an interagenacy agreement between the NCSC and FAA which was signed in February 1986 (attached). An amendment to the agreement was necessary in order to extend the coverage of funds to fiscal 1987 and covered a trip during the period 29 September 1986 through 3 October 1986 (attached).

All direct support to the FAA was provided prior to 29 October 1986 when NTISSP # 2 was signed. NTISSP # 2 did not have any effect on the agreement or the subsequent support provided.

US Department
of Transportation

Federal Aviation
Administration

800 Independence Ave. S.W.
Washington, D.C. 20591

26 NOV 1985

Dr. Robert Brotzman
Director
National Computer Security Center
9800 Savage Road
Fort George E. Meade, Maryland 20755

Dear Dr. Brotzman:

This is in reference to the October 22 meeting between Messrs. Leon Cooper and Dave Jones of your organization, and Mr. William L. Riggle of my staff. During this meeting, the application of the Department of Defense Trusted Computer System Evaluation Criteria (Report CSC STD-001-83) to the Federal Aviation Administration (FAA) Air Traffic Control (ATC) System was discussed.

In accordance with suggestions received at the above meeting, it is requested that your organization provide advice and assistance in the following areas:

1. The review and evaluation of the current security status of:

    a. FAA's present ATC system (IBM 9020 Computers);
    b. FAA's new "Host" computer system (IBM 3083); and
    c. FAA's proposed Advance Automation System (to be determined).

2. The development and presentation of:

    a. ADP security training courses;
    b. ADP security awareness briefings; and
    c. ADP threat briefings.

3. The application of report CSC-STD-001-83 to all FAA computer systems.

4. The development of standards and guidelines for:

    a. Software security (passwords, audit trails, etc);
    b. Administrative security procedures; and
    c. Contingency plans.

5. The review and evaluation of FAA's risk analysis methodology and ADP risk analysis reports.

6. The review and evaluation of FAA's methodology for certification of sensitive applications (payroll, personnel system, etc.)

The above effort will require travel by your personnel to Atlantic City, New Jersey; Oklahoma City, Oklahoma; Seattle, Washington; Albuquerque, New Mexico; and possibly other locations.

It is anticipated that your support will be required through fiscal year 1986. We are in the process of recruiting additional ADP security specialists in our Washington headquarters and each of our nine regions and two research centers.

If this proposal is acceptable to you, we will take the necessary steps to develop an interagency agreement to cover the financial arrangements.

If there are any questions, please contact Mr. William L. Riggle, FAA National ADP Security Program Manager, 202/426-3038.

Sincerely,

Billie H Vincent

Billie H. Vincent
Director of Civil Aviation Security

Interagency Agreement No.
DTFA01-86-Z-02014
Page 1 of 2

INTERAGENCY AGREEMENT
BETWEEN
DEPARTMENT OF TRANSPORTATION/FEDERAL AVIATION ADMINISTRATION
AND
THE NATIONAL SECURITY AGENCY/NATIONAL COMPUTER SECURITY CENTER
FOR TECHNICAL SUPPORT FOR FAA COMPUTER SECURITY PROGRAM

I. STATEMENT OF WORK

The National Computer Security Center (NCSC) will assist the Federal Aviation Administration (FAA) in the following projects:

1. The review and evaluation of the current security status of:
   a. FAA's present ATC system (IBM 9020 Computers);
   b. FAA's new "host" computer system (IBM 3083); and
   c. FAA's proposed Advanced Automation System (to be determined).
2. The development and presentation of:
   a. ADP security training courses;
   b. ADP security awareness briefings; and
   c. ADP threat briefings.
3. The review and evaluation of FAA's methodology for certifcication of sensitive applications (payroll, personnel system, etc.).
4. The review and evaluation of FAA's risk analysis methodology and ADP risk analysis reports.

The above effort will require travel by NCSC personnel to Atlantic City, New Jersey; Oklahoma City, Oklahoma; Seattle, Washington; and possibly other locations.

Interagency Agreement No.
DTFA01-86-Z-02014
Page 2 of 2

II. PERIOD OF PERFORMANCE AND DELIVERY SCHEDULE

The period of performance for this effort will be through September 30, 1986.

Upon completion of each project or subproject, the NCSC will deliver a letter report to the FAA in accordance with the following schedule:

Project	Due Date
1a.	July 30, 1986
1b.	August 30, 1986
1c.	September 30, 1986
2a.	June 30, 1986
2b.	May 30, 1986
2c.	May 30, 1986
3.	August 30, 1986
4.	July 30, 1986

III. PLACE OF DELIVERY

The reports to be delivered hereunder will be delivered to the following address:

Federal Aviation Administration
Office of Civil Aviation Security
800 Independence Avenue, SW
Washington, DC 20591
Attention: William L. Riggle, ACS-320

IV. FUNDING AND REIMBURSEMENT

The total estimated amount funded hereunder is $9,000 to cover travel expenses. There will be no charges for labor, overhead, or other costs.

An advance of funds may be requested via SF-1080, citing appropriation 601.0/4540/460/2591 and this Interagency Agreement No. These references shall be cited on all correspondence relating to fiscal and contractual matters. SF-1080 shall be submitted to the Accounts Payable Branch, AAA-220, 800 Independence Avenue, SW, Washington, DC 20591, who will make payment thereon.

V. AUTHORITY

This agreement is entered into pursuant to the authority of 49 U.S.C. 322(c)(I).

AGREED:

National Computer Security Center
By: R A Cavaluchi
ROBERT A. CAVALUCHI, CDR USN
Title: Applications Systems Evaluati
Date: 25 February 1986

Federal Aviation Administration
By:
JOHN R. DUPREE
Title: CONTRACTING OFFICER
Date: 2/10/86

Amendment No. 0001
Interagency Agreement No.
DTFA01-86-Z-02014

AMENDMENT

TO

INTERAGENCY AGREEMENT
BETWEEN
DEPARTMENT OF TRANSPORTATION/FEDERAL AVIATION ADMINISTRATION
AND
THE NATIONAL SECURITY AGENCY/NATIONAL COMPUTER SECURITY CENTER
FOR TECHNICAL SUPPORT FOR FAA COMPUTER SECURITY PROGRAM

This amendment is to extend the period of performance to 1 November 1986 as specified in Interagency Agreement No. DTFA01-86-Z-02014, covered by SF-1080, appropriation 6961301/4540/460/2591 in order to complete the final project begun on 28 September 1986.

The total value of this agreement remains at $9,000.

AGREED:

NATIONAL COMPUTER SECURITY CENTER

By:
ROBERT A. CAVALUCHI, CDR USN
Title: AIS Evaluations
Date: 03 OCT 1986

FEDERAL AVIATION ADMINISTRATION

By:
JOHN R. DUPREE
Title: CONTRACTING OFFICER
Date: 10/3/86

P.R. No.: 87-08906
T.O.: William Riggle, ACS-320

QUESTION: Has NSA conducted any visits to Mead Data Central in the last year concerning NSDD-145 and NTISSP No. 2?

ANSWER: No

QUESTION: Has NSA conducted any visits to Mead Data Central in the last year?

ANSWER: We are aware of at least one trip to Mead Data Central made by an Intelligence Community Information Handling Committee (IHC) team that included the NSA IHC Representative. The team visited Mead Data on the afternoon of 29 September 1986. The stated purpose of the visit was twofold and the principal Mead participants were Mr. Gerald E. Yung, Vice President and General Counsel, and Mr. Robert S. Willard, Director, Government Markets. The primary purpose was to obtain the technical details, to include size, programming language, etc., of the software used by Mead to provide LEXIS-NEXIS service in order to evaluate its potential for use in a different application along with a determination of Mead's willingness to license or otherwise sell the software. A secondary purpose was to explore the willingness of Mead to license or otherwise sell a copy of the software and the NEXIS data bases (with updates) to allow an agency or group of agencies to run the system on a protected system to permit greater user access to such data bases. Efforts such as these are now relatively common by both large private sector entities as well as government entities at various levels. At no time during these discussions were issues related to access by other countries to Mead products or issues related to sensitive but unclassified data discussed. Mead indicated that they did not license or market their software at present but would undertake a corporate review to determine whether they wished to discuss the matter further. Sometime later a Mead representative indicated that the NSA representative and two Agency software experts were invited to visit Mead on the morning of 26 February 1987 as Mead would like to further explore the Agency's requests. That meeting was cancelled by Mead on 24 February 1987 due to Mead's appearances before the House Government Operations Committee and the House Science, Space and Technology committee. Mead has offered alternative dates in May 1987 for this meeting and a firm date is being coordinated.

QUESTION: Can NSA estimate the costs that have resulted from computer security losses?

ANSWER: We have no credible data in this area. We believe that some data relating to auditable losses might be available from IGs. Much of the loss of computer use or data which we observe is not auditable and is either unreported by the system operator or unknown to him.

Although we believe these losses are significant, we are unable to provide any aggregate data. All our knowledge consists of examples, most of which are provided to us by the system operators. In cases where we obtain this information as part of our Security support, we must respect the confidentiality of this data.

Mr. McCurdy. The next witness is Mr. Raymond Kammer, Deputy Director, National Bureau of Standards, and he is accompanied by Mr. James Burrows, Director of the Institute for Computer Science and Technology, the National Bureau of Standards.

I would advise members of the subcommittees that we have at least nine more witnesses, and we need to probably on the next group combine them in a panel and save our questions until they've each summarized their materials.

We will have a panel of four and then a panel of three.

It's good to see you again Mr. Kammer. We worked together some time ago, and I appreciated your work there. Your testimony will be submitted—admitted into the record in its entirety, and we look forward to hearing you and Mr. Burrows.

STATEMENT OF RAYMOND G. KAMMER, DEPUTY DIRECTOR, NATIONAL BUREAU OF STANDARDS, ACCOMPANIED BY JAMES H. BURROWS, DIRECTOR, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY, NATIONAL BUREAU OF STANDARDS

Mr. Kammer. Thank you, sir, Mr. McCurdy, Mr. Walgren.

Mr. McCurdy. You need to pull that mike a little closer.

Mr. Kammer. Okay, how's that?

Mr. McCurdy. That's great. Thank you.

Mr. Kammer. As my testimony will be in the record, I will confine myself to just a couple remarks.

The Administration doesn't have a position on H.R. 145 yet, but we in the Department of Commerce are looking forward to working with this committee to develop a final product that we hope everyone will be able to support.

The rest of my testimony is concerned with pointing out aspects of the H.R. 145 that we support and some other aspects where we'd recommend changes. I think it's fair to say that the changes that we are recommending are not the philosophy, but rather to some of the implementation approaches.

In addition, in my testimony, I highlight some notable accomplishments by ICST with respect to computer security, and I have included in the testimony as an attachment a more extensive description of that.

Rather than go through all of that now, I'll just close there, and we'll take questions, if you all have any.

Mr. McCurdy. Mr. Burrows, any comments or a statement for the record?

Well, thank you. That's nice.

Mr. McCurdy. As a representative of the Department of Commerce and the Administration, I would admonish you, the same way I did General Odom, and that is to take a message back that again there is a small window of opportunity here. I think it's important, if you want to have input, that it be made rather quickly, and that the principals who can affect that are here and reside with also Mr. Brooks and his committee, and we look forward to working with you.

Mr. Glickman.

Mr. Glickman. Well, first of all, thank you for appearing today.

In connection with your testimony before the previous Congress, I take this to be much more supportive than what you had testified before; is that a fair statement?

Mr. **Kammer**. Yes, sir. It was intended to be more supportive, Mr. Glickman.

Mr. **Glickman**. Because I would just read that you say in your statement:

> While I must point out that the Administration has not established a position on H.R. 145, I personally look forward to working with the committee to develop an effective computer security bill.

You talk about the bill has some positive features. You talk about some things which you want changed. From a philosophical point of view, you do not have a problem with the legislation.

Mr. **Kammer**. No, sir.

Mr. **Glickman**. What changed your mind?

Mr. **Kammer**. When last the Department of Commerce was testifying, which was the Deputy Secretary of Commerce and me, we didn't know about the Poindexter Directive.

Mr. **Glickman**. I'm sorry. You didn't——

Mr. **Kammer**. We didn't know about the Poindexter Directive. And when NSDD–145 was being drafted, there was quite a bit of discussion, in fact dispute, over the governance that 145 would have. What it would apply to and what it wouldn't apply to.

It was our belief that 145 did not apply to civil data, the civil computer systems that the Brooks Act and the Privacy Act have delegated to the Bureau of Standards.

The definition of sensitive data that's contained in the Poindexter Directive is a totally—in my point of view, at least—is a totally inclusionary definition. There is no data that anyone would spend money on that is not covered by that definition. Therefore, civil data is covered; therefore, the Brooks Act and the Privacy Act are either in conflict with it, or one is superior to the other.

I have a conflict. I would like to see a resolution. I think this legislation does it.

Mr. **Glickman**. Well, you basically would take the position that the definitional standards in the Poindexter Memorandum relating to the nature of the data is potentially—would potentially include civil information, non-military information?

Mr. **Kammer**. I believe it does, sir.

Mr. **Glickman**. It does contain civil information.

Mr. **Kammer**. With the definition of "sensitive, but non-classified data" that comes out of the Poindexter Directive.

Mr. **Glickman**. Now I think it was General Odom and Mr. Latham that testified that there's not much difference between the definitions in the bill and the Poindexter Memorandum.

How would you respond to that?

Mr. **Kammer**. The definitions in the bill and in the Poindexter Memorandum are virtually the same; however, the application, the intent with which that definition is used are quite different.

In the one case, one assumes that the next step is—all data now that is kept in databanks is at least sensitive, but non-classified, or virtually all. The next logical step after that is to prescribe access-limiting procedures and require their application.

The intent of the legislation, as I understand it, the next step after having defined what sensitive data is, is to develop a set of tools and make them available to people to use at their discretion. I see that as a difference, and to my mind, an important difference.

Mr. **Glickman**. Well, you do state in your statement in the third paragraph:

> The bill removes the potential for conflict between the Department of Commerce and the Director of the NSA in its capacity as national manager under the directive. Conflict has not yet arisen because the level of cooperation is satisfactory.

Mr. **Kammer**. We've worked very well with NSA, and they have a lot of skills that we don't have, never will have, shouldn't have. And they've been very generous in making them available to us. Particularly—it seems reasonable, I'm sure, to everybody, the Department of Defense and NSA in particular will assign a higher value and therefore be more vigorous in their research in computer security, because they have a lot more to protect.

They have shared that information with us in an appropriate way, and we enjoy working with them.

Mr. **Glickman**. Okay. Well, Mr. Chairman, because of time, I will not ask any more questions.

I appreciate the candor of your testimony, and I think it's important, and I'm hopeful again, as the chairman of the subcommittee, that we would get at some of the specifics. I note we have a problem still with the definition in the bill, and we need to get at some of the specifics of the problem.

Thank you.

Mr. **McCurdy**. The gentleman from Missouri?

Mr. **Buechner**. The only thing I would like to add is that if you would like to give us a definition of "sensitive" that you think would be the most usable one to cover both federal and civilian, I think we'd appreciate that.

Mr. **Kammer**. We're willing to try. I will say that it's very—I have yet to see a definition that doesn't either fail to do the job or create an uneasy feeling that we're doing something to the public's access to data. It's an illusive concept.

Mr. **Buechner**. I know. Before I got married, I always had a difficult time in defining "sensitive." [Laughter.]

Thank you, gentlemen.

Mr. **McCurdy**. Mr. Kammer, quickly, what additional resources would you require to carry out H.R. 145, and also are you comfortable that you could carry out the responsibilities in the bill?

Mr. **Kammer**. I'll answer the easier question first. Yes, I am comfortable that we can carry out the responsibilities, and Mr. Burrows may want to comment more extensively on that. He is in charge of that area.

With respect to resources, our suggestion that I've outlined in my testimony is that we approach this as a reimbursable service, and therefore the cost of making a computer bank more secure will rest with the people who are the maintainers of that computer bank.

That's appealing to me because I think that computer security should be a part of the cost of doing business for everybody, and they do reap benefits as well as spend money on this.

My estimate is—our current expenditure is $1 million in direct funds and about $550,000 in funds transferred from other agencies, of which $150,000 of that $550,000 comes from NSA.

My best estimate is that we would need a program on the order of $5 or $6 million to respond to the Government as a whole, the civil Government as a whole. So, our reimburseable program would have to increase five, perhaps a factor of eight or ten.

Mr. McCurdy. Thank you. Mr. Walgren?

Mr. Walgren. Thank you, Mr. Chairman.

You mentioned that you are attracted to this by its reimburseable nature and yet the structure of the bill is that we would be doing certain things centrally and then agencies could or could not reach out and pick this up.

How do you reconcile then the fact that there would be central costs, obviously, I gather, in developing the standards and the expertise and the like which then may or may not be distributed over the universe of Federal computers and if it were not distributed over everybody, then those agencies that chose to come in and pick it up would be paying a substantial amount of central overhead that would be more—larger.

Mr. Kammer. Well, as you know, sir, we are constantly juggling that problem. Our other agency budget is about $80 million in comparison to our direct appropriated budget of about $120 million. There is always sort of the chicken and egg problem, how to you develop the resource that people will then pay for.

Mr. Walgren. Yes. Let me ask you this. As I understand it, this is a pretty big task when you consider the Government as a whole, and that's one of the reasons that we are not able to mandate that everybody jump into the pool and do it. We want to go forward somewhat tentatively, but would you describe the Bureau of Standards as one of those agencies that General Odom characterized that was unable to draw attention to the need for certain kinds of funding that then the military as in the National Security Agency here, had to come in and do what amounted to a civilian service?

Mr. Kammer. We have not experienced budget growth in the computer area including computer security.

Mr. Walgren. In fact, the experience is the lack thereof——

Mr. Kammer. It's been shrinking.

Mr. Walgren. In tremendous dimension.

Let me ask you one other thing. What the military has to do for the military is a little different, wouldn't it be, than what we probably would logically do for the civilian side inasmuch as with the kind of information they are trying to protect, the cost would be no object, and yet cost would be very much an object for the degree of security that we would be building into the wide range of non-sensitive or even sensitive data handling.

Mr. Kammer. That's very much the case, both for the private sector generally in their non-defense pursuits, at least, and for the civil agencies. There is a value you can assign to the data. In the national security case, the value is without limit but in most civil cases, there is a value and one doesn't want to invest in more protecting something than its worth.

Mr. Walgren. Thank you, Mr. Chairman.

Mr. McCurdy. I thank the gentleman from Pennsylvania. The gentleman from Maryland had to leave but he had a question that he wanted submitted, and that was why NBS opposed the Privacy Board. Is it in fact that you do oppose the Privacy Board and if so, why?

Mr. Kammer. Sir, we have a statutory visiting committee already which meets twice a year and advises us and the Secretary of Commerce on our activities. We also pay the National Academy of Sciences and National Academy of Engineering to convene some 15 independent boards, people from the private sector and academic community primarily, to come in and review the Bureau of Standards, which they do.

I don't feel lack of advice already, to be very honest. I am not sure that I may not have reached my capacity to take advice.

Mr. Buechner. Mr. Chairman.

Mr. McCurdy. Yes.

Mr. Buechner. Mr. Kammer, I think it is safe to say that this Committee would expect the Administration to sort of get its act together and to come forward in an unified manner and that Commerce and Defense would get together so that we are not getting this stereophonic sound, but the difference is that each speaker has a different tune.

So, if you would convey that message to whoever it is filling your capacity to take advice, I would appreciate it. I think the Committee as a whole would also.

Mr. McCurdy. The gentleman's point is well taken. We certainly appreciate that input. I think the process has—because the bill came on the Floor rather suddenly last year, that the process of debate was healthy and I think we are finally getting there. It was either Madison or Hamilton, I recall, in one of the Federal's papers that said "to promptitude a decision in the legislature is more often an evil than a benefit." I think we have gained something here, and hopefully the time and real clear thinking and people getting together is going to assist us in having a better bill.

Mr. Kammer, Mr. Burrows, thank you very much. We will proceed with the next witnesses.

[The prepared statement of Mr. Kammer follows:]

U.S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS
STATEMENT OF MR. RAYMOND G. KAMMER
DEPUTY DIRECTOR
BEFORE THE SUBCOMMITTEES ON
SCIENCE, RESEARCH AND TECHNOLOGY
AND TRANSPORTATION, AVIATION AND MATERIALS
U.S. HOUSE OF REPRESENTATIVES
FEBRUARY 26, 1987

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

THANK YOU FOR THIS OPPORTUNITY TO TESTIFY TODAY ON THE TOPIC OF COMPUTER SECURITY. I AM ACCOMPANIED BY MR. JAMES BURROWS, DIRECTOR OF THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY AT THE NATIONAL BUREAU OF STANDARDS.

I AM HERE TODAY TO REPRESENT THE DEPARTMENT OF COMMERCE VIEWS ON H.R. 145 AND TO REPORT ON RECENT COMPUTER SECURITY ACTIVITIES AND ACCOMPLISHMENTS WITHIN THE DEPARTMENT OF COMMERCE AT THE NATIONAL BUREAU OF STANDARDS. I HAVE ATTACHED TO MY TESTIMONY A MORE EXTENSIVE DESCRIPTION OF THE NBS COMPUTER SECURITY ACTIVITIES.

COMMENTS ON H.R. 145

WHILE I MUST POINT OUT THAT THE ADMINISTRATION HAS NOT ESTABLISHED A POSITION ON H.R. 145, I PERSONALLY LOOK FORWARD TO WORKING WITH THE COMMITTEE TO DEVELOP AN EFFECTIVE COMPUTER SECURITY BILL. FROM THE DEPARTMENT OF COMMERCE VIEW, H.R. 145 HAS SOME POSITIVE PROVISIONS. H.R. 145 DELEGATES THE PRIMARY RESPONSIBILITY FOR THE SECURITY OF SENSITIVE BUT UNCLASSIFIED INFORMATION TO FEDERAL AGENCIES AND OTHER ORGANIZATIONS WHICH PROCESS COMPUTER DATA ON BEHALF OF THE FEDERAL GOVERNMENT. THE DEPARTMENT OF COMMERCE FULLY SUPPORTS THIS DELEGATION OF AUTHORITY.

THE BILL SPECIFIES THAT THE NBS STUDY COMPUTER TECHNOLOGY AND ITS VARIOUS APPLICATIONS. IN ADDITION TO DEVELOPING STANDARDS AND GUIDELINES FOR COMPUTER SECURITY. THIS ASSIGNMENT CONFIRMS FUNCTIONS THAT THE NBS ALREADY PERFORMS. THE DEPARTMENT SUPPORTS THE CONTINUED NBS ROLE IN COMPUTER RESEARCH AND RELATED STANDARDS DEVELOPMENT.

THE BILL REMOVES THE POTENTIAL FOR CONFLICT BETWEEN THE DEPARTMENT OF COMMERCE AND THE DIRECTOR OF THE NATIONAL SECURITY AGENCY (NSA) IN HIS CAPACITY AS NATIONAL MANAGER UNDER NATIONAL SECURITY DIRECTIVE 145 (NSDD 145). CONFLICT HAS NOT YET ARISEN BECAUSE THE LEVEL OF COOPERATION BETWEEN NBS AND THE NATIONAL MANAGER TO DEVELOP SECURITY STANDARDS HAS BEEN SATISFACTORY. WE HAVE WORKED WELL TOGETHER.

THE DEPARTMENT OF COMMERCE HAS TWO DELEGATIONS OF AUTHORITY FOR COMPUTER SECURITY. THESE ARE PUBLIC LAW 89-306 (BROOKS ACT) AND EXECUTIVE ORDER 11717. NSDD 145 ASSIGNS TO THE NATIONAL MANAGER AUTHORITY FOR "...REVIEWING AND APPROVING ALL STANDARDS, TECHNIQUES, SYSTEMS, AND EQUIPMENTS FOR TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY." HOWEVER, NSDD 145 SPECIFICALLY STATES THAT IT IS NOT INTENDED TO "...AMEND OR CONTRAVENE THE PROVISIONS OF EXISTING LAW, EXECUTIVE ORDERS, OR PRESIDENTIAL DIRECTIVES WHICH PERTAIN TO THE PRIVACY ASPECTS OR FINANCIAL MANAGEMENT OF AUTOMATED INFORMATION SYSTEMS..."

THERE ARE OTHER ASPECTS OF THE BILL WHICH WE DO NOT SUPPORT. THE BILL DOES NOT PROVIDE SUFFICIENT GUIDANCE OR DEFINITION ON THE TYPE OF INFORMATION THAT IS TO BE CONSIDERED "SENSITIVE, BUT UNCLASSIFIED". AS A RESULT, TOO MUCH OR TOO LITTLE INFORMATION MAY RECEIVE PROTECTION. IN ADDITION, THE DEPARTMENT CANNOT ESTIMATE THE NUMBER OF SYSTEMS FOR WHICH NBS MAY BE ASKED TO PROVIDE ASSISTANCE AND TRAINING MATERIALS. ALTHOUGH NBS ALREADY PERFORMS THESE FUNCTIONS, THE BILL MAY EXPAND THE NUMBER OF AGENCIES WHICH REQUEST THIS ASSISTANCE. WE CANNOT THEREFORE EVALUATE THE ADMINISTRATIVE OR FINANCIAL BURDEN WHICH MAY BE CREATED. WE RECOMMEND THAT THE BILL CLARIFY THE EXISTING AUTHORITY OF NBS TO PERFORM THESE SERVICES ON A COST REIMBURSABLE BASIS.

ADDITIONALLY, WE OPPOSE THE ADDITION OF A COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD WITHIN THE DEPARTMENT. NBS ALREADY HAS ADEQUATE MECHANISMS FOR EXTERNAL ADVISE. THESE INCLUDE THE NBS VISITING COMMITTEE AND THE BOARD OF ASSESSMENT OF NBS PROGRAMS TO THE BUREAU MANAGEMENT AND TO THE DEPARTMENT. ANOTHER ADVISORY COMMITTEE WOULD BE UNNECESSARY AND COSTLY.

WE OPPOSE THE BILL'S REQUIREMENT THAT EACH WAIVER OR DELEGATION OF AUTHORITY RESPECTING STANDARDS ISSUED UNDER THE BROOKS ACT BE TRANSMITTED TO THE HOUSE COMMITTEE ON GOVERNMENT OPERATIONS AND THE SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS. IF THE COMMITTEES WISH TO BE INFORMED OF SUCH ACTIONS, WE SUGGEST AN ANNUAL REPORT RATHER THAN IMMEDIATE NOTIFICATION OF THESE MANAGERIAL DECISIONS.

FINALLY, WITH REGARD TO SECTION 5 OF THE BILL WE CAN SEE NO NEED FOR OPM TO HAVE TO ISSUE TRAINING REGULATIONS TO IMPLEMENT TRAINING GUIDELINES NBS WILL BE ISSUING. AND WE UNDERSTAND OPM ALSO OBJECTS TO THIS REQUIREMENT, PARTICULARLY IN SO FAR AS IT WOULD INVOLVE OPM IN REGULATING TRAINING FOR PRIVATE CONTRACTORS OR EMPLOYEES RATHER THAN GOVERNMENT EMPLOYEES. WE BELIEVE THAT EACH GOVERNMENT AGENCY SHOULD BE RESPONSIBLE FOR IMPLEMENTING ITS OWN TRAINING PROGRAM.

COMPUTER SECURITY ACCOMPLISHMENTS

THE NBS INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY COMPUTER SECURITY DIVISION DEVELOPS, VALIDATES, AND MAINTAINS SECURITY STANDARDS FOR THE FEDERAL GOVERNMENT. FOR EXAMPLE, NBS PLAYED A MAJOR ROLE IN DEVELOPING THE INTERNATIONALLY ACCEPTED OPEN SYSTEM INTERCONNECTION (OSI) NETWORK SECURITY SYSTEM ARCHITECTURE WHICH PROVIDES THE FRAMEWORK FOR THE DEVELOPMENT OF STANDARDS FOR INTERCONNECTING A SET A COMPUTER SYSTEMS THAT ARE MANUFACTURED BY DIFFERENT VENDORS. RECENTLY, NBS HAS BEGUN DEFINING THE SECURITY COMPONENTS OF THE OSI ARCHITECTURE. WITHIN THAT SCOPE, THE DIVISION IS DEFINING, IMPLEMENTING, DEMONSTRATING, AND TESTING SECURITY STANDARDS. THESE STANDARDS PROVIDE WORLD-WIDE SECURITY SERVICES FOR PROTECTING DATA AGAINST UNAUTHORIZED MODIFICATION, UNDETECTED DATA LOSS, AND UNAUTHORIZED DISCLOSURE, AS WELL AS VERIFICATION OF THE IDENTITIES OF BOTH THE SENDER AND RECEIVER OF COMPUTER DATA.

IN PARALLEL WITH THE OSI SECURITY EFFORT, THE NBS COMPUTER SECURITY DIVISION HAS CONTINUED TO DEVELOP AND VALIDATE SECURITY STANDARDS FOR FINANCIAL DATA NETWORKS. THE DIVISION PROVIDES TECHNICAL CONSULTATION AND PRODUCES GUIDELINES AND STANDARDS TO ASSIST OTHER FEDERAL AGENCIES AND MEMBERS OF THE PRIVATE SECTOR IN THE EVALUATION OF THEIR SECURITY NEEDS AND PROVIDES RECOMMENDATIONS FOR SYSTEM IMPLEMENTATIONS AND MODIFICATIONS. I HAVE ATTACHED A MORE EXTENSIVE SUMMARY OF THE EFFORTS OF THE NBS

COMPUTER SECURITY DIVISION TO MY TESTIMONY. THANK YOU FOR YOUR ATTENTION. I WOULD NOW BE HAPPY TO RESPOND TO ANY QUESTIONS YOU THAT MAY HAVE.

Institute for Computer Sciences
and Technology
National Bureau of Standards

Computer Security Activities

I. INTRODUCTION

Since the early 1970s, ICST has been responsible for a telecommunications and computer security program. This program has focused on the development and transfer of cost-effective solutions for protecting automated information -- both that which is processed and stored by computers and that which is transferred between computer systems. The program was originally established to assist the Federal agencies. However, ICST has always worked directly with private sector users and vendors and through the voluntary standards process to disseminate solutions that are applicable to a broad spectrum of users.

This technology-based program has produced numerous management and technical publications as well as conferences, workshops, seminars, and other technology transfer activities. The following are some of the many ICST security-related publications that have been used widely in Government and the private sector.

Guidelines for ADP Physical Security and Risk Management, FIPS-PUB-31.

Data Encryption Standard, FIPS-PUB-46.

Guidelines for Automatic Data Processing Risk Analysis, FIPS-PUB-65.

Guidelines for Security of Computer Applications, FIPS-PUB-73.

Guidelines for ADP Contingency Planning, FIPS-PUB-87.

Guideline for Computer Security Certification and Accreditation, FIPS-PUB-102.

Standard on Password Usage, FIPS-PUB-112.

Standard on Computer Data Authentication, FIPS-PUB-113.

Security of Personal Computer Systems: A Management Guide, NBS Special Publication 500-120.

Security of Dial-Up Lines, NBS Special Publication 500-137.

Continuing ICST telecommunications and computer security activities address important technical and management issues and foster close cooperative relationships between the Federal and private sectors. The following are highlights of ICST's current technical, laboratory-based efforts in the areas of security technology and security management.

II. SECURITY TECHNOLOGY

The objective of ICST's security technology effort is to improve the security of Government computer networks by developing, validating, and maintaining security standards. This effort has four components which are discussed below.

Open System Interconnection (OSI) Network Security

The Open Systems Interconnection Architecture, which has been adopted as an International Standard (ISO 7498), provides the framework for the development of standards for interconnecting a set of computer systems manufactured by different vendors, both domestic and foreign. ICST has played a major role in developing the OSI Architecture and in fostering its domestic and international acceptance. Recently, ICST has turned its attention to defining the security components of the OSI architecture, and within that scope, defining, implementing, demonstrating and testing security standards. These standards would provide common, world-wide security services for protecting data against unauthorized modification, undetected loss, and unauthorized disclosure, as well as verification of the identities of both the sender and receiver of data.

ICST also is working with the National Security Agency to assure that security standards developed within the OSI Architecture will, to the extent possible, also meet Department of Defense requirements for protecting classified and intelligence data throughout their Secure Data Network System.

Other Network Security Standards

In parallel with the OSI Security Architecture effort, ICST has continued to develop and validate security standards for financial data networks and to advise Government agencies on secure network implementations. Specific activities include:

- A continuing work agreement with the Department of Treasury to develop validation criteria and to implement validation systems for determining if vendors' products correctly implement standards for message authentication and key management. In addition, ICST is assisting Treasury in developing the security requirements and specifications for a new system that will certify requests from Federal agencies for direct electronic funds payments from Treasury to Government contractors.

Network Cryptography

The increased use of computer networks has led to a corresponding increase in the need for cryptographic security. In the near future, complete business transactions between buyer, seller, and banker will be performed electrically with automated communications. In most cases, cryptography provides the only effective means to prevent eavesdropping and alteration of these transmissions.

In anticipation of the increased use of computer networks, NBS developed the Data Encryption Standard (DES) in 1977. This was followed by a series of related FIPS standards and guidelines for the purpose of protecting unclassified, but valuable or sensitive information. The acceptance and use of DES has grown steadily and continues to be widely used almost ten years after its promulgation. Many organizations, including the banking community and several Federal agencies, have made large investments in DES technology.

To support the use of DES throughout the Federal and private sectors, ICST validates commercial devices for correct implementation of the DES algorithm and conducts periodic reviews of the DES to assure that it affords continued protection to computer information. When purchasing a devices validated by ICST, consumers are assured that the devices were designed properly and that they are compatible with other devices that implement the standard. Developers of devices have a stable standard which they can incorporate into a variety of products and sell to users in government and the private sector. ICST expects to announce the second review of DES in the Federal Register in early 1987.

III. COMPUTER SECURITY MANAGEMENT

The Computer Security Management activity is responsible for developing guidance in a broad range of areas affecting the overall assessment and management of computer security risks. The elements of this program are the following:

Personal Computer Security

ICST has provided important technical and management guidance to the rapidly increasing universe of personal computer system users. This guidance includes the issuance of an NBS Special Publication, Security of Personal Computer Systems: A Management Guide, which has been widely used in both the government and private sectors. Additional work continues in the examination of new security technologies applicable to personal computers and local area networks.

System Security

ICST conducts research in various hardware and software technologies that provide automated system access control and security. A recent publication, Security for Dial-Up Lines, provided a detailed guide to the selection of systems to protect computer systems from unauthorized access by outside (dial-up) users. Work is continuing in such areas as UNIX/POSIX security standards and the application of artificial intelligence technology to system security.

Security Audit and Evaluation

Security methods and technologies must be intelligently designed, implemented, and managed. Indeed, this process itself requires systematic techniques. ICST has long been involved in activities to advance the "state-of-the-art" is security audit and evaluation techniques. Specific activities in progress include:

Guideline for Security in the System Development Life Cycle - As part of a joint effort with the President's Council on Integrity and Efficiency (PCIE), ICST has participated in the development of guidance for ensuring the inclusion of security, audit, and control mechanisms in systems throughout the systems life cycle.

Security Event Logging - NBS is developing a FIPS standard for the recording of security-significant events in computer systems. This standard will help ensure that minimum audit trail data is available for all computer systems in which sensitive or critical data is maintained.

Laboratory Activities

Computer security standards and guidance must be based on an understanding of both the risks and opportunities provided current and developing technologies. Analysis of these technologies is the purpose of the ongoing ICST information security laboratory research program.

In an effort to make research findings available, ICST publishes special publications, internal reports, and technical papers on various aspects of laboratory research activities. In addition, we maintain a Security Products Database containing information on a wide range of available computer and telecommunications security products. This and other information are disseminated through the Security Bulletin Board, an electronic bulletin board system available to anyone in Government or the private sector.

Related Efforts

In addition to the major programs outlined above, cooperative efforts are undertaken with other agencies of Government to assist in both the development and dissemination of computer security management methods.

Small Business Computer Security Guide - As part of NBS' official role on the Small Business Security & Education Advisory Council, we developed a concise guideline on computer security for the owners of small businesses. The purpose of this guide is to provide clear and practical computer security guidance for this special class of computer users.

Intelligence Community Staff - NBS' computer security efforts normally do not address the protection of national security information. However, at the request of the Intelligence Community (IC) Staff, we developed a booklet entitled Processing Intelligence Information on Personal Computers. This booklet provides users with basic guidance on the protection of highly sensitive intelligence information in personal computer systems.

Security Components Standards - We are participating in a working group chaired by the National Computer Security Center for the development of formal evaluation criteria for computer security components or subsystems. This effort should enable more objective evaluation and selection of security subsystems which can increase the protection of existing systems.

Other Agency Support - We have worked with several agencies on special projects involving the practical application of computer security technologies and management methods. These projects have often involved participation in reviews or other risk assessments of sensitive systems or applications.

IV. FUTURE ACTIVITIES

As technology changes and the use of computer and communications technology increases, there will be greater demand -- in Government and the private sector -- for additional tools in protecting vital and sensitive information. ICST plans to continue to fulfill is responsibility to provide relevant, cost-effective solutions the nation's automated information system (AIS) security needs. The following are some of the areas in which FIPS Guidelines, and other publications are planned.

Automated Authentication Techniques - There exists a wide variety of technical methods for authenticating the identity of a user or other element in a computer system or network. However, there is a need for specific and consistent guidance for the evaluation, selection, and use of such methods.

Access Authorization and Control - As more types of computer systems and networks are interconnected, there is an increasing need for standard methods for granting and controlling access to system resources.

Automated Information System Security Management - The first FIPS publication on computer security (FIPS 31) has provided thousands of managers in Government and industry with the basic concepts for effective computer security management. That publication was issued over a decade ago and needs revision for the new, more complex, and more decentralized information system environment of today and the future.

Glossary for AIS Security - An early FIPS publication (FIPS 39) is still the standard glossary for computer security. However, several new terms and conflicting terminology have developed since its publication, and an updated glossary is needed.

Application of Cryptography to AIS Security - Cryptography is often seen primarily as a communications security measure (i.e., to protect information in transit. However, it also has an important role in the protection of stored information, such as in personal computers and other systems that cannot be physically protected.

Risk Analysis - The basis for all decisions regarding the design and implementation of security measures is some assessment of risks and benefits of controls. Additional guidance is needed for the increasing number of users and managers who must make these decisions.

AIS Contingency Planning (Network) - The use of telecommunications networks to connect users and computers increases the potential for disaster if elements in such networks are disabled. Guidance is needed for managers to plan for such contingencies.

Artificial Intelligence Applications in AIS Security - As computer and telecommunications systems become more complex, so does the problem of monitoring their activities, analyzing their vulnerabilities, and selecting appropriate control measures. Rapidly developing artificial intelligence (AI) technologies provide a promise to aid in these and other security problems.

V. SUMMARY

For more than a decade, NBS' Institute for Computer Sciences and Technology has played an important and leading role in developing an awareness of the need for computer and telecommunications security throughout Government and industry -- and in developing the technology, standards, and guidance needed to provide that security. Although the ICST computer and telecommunications security program is officially targeted at the non-national-security segment of the Federal Government, the program's benefits have been realized in the private sector as well. Government and industry have looked with confidence to ICST for relevant, cost-effective solutions to their computer and communications security needs. We hope that our current and future efforts -- in the laboratory, in national and international standards organizations, in our publications, and in the information security community -- will continue to provide the solutions and guidance needed in an ever more complex and vital information-based world.

Mr. McCurdy. The next witnesses will be a panel of Mr. Jack Simpson from Mead Data Central, Inc., accompanied by Mr. Kenneth Allen, also Ms. Cheryl Helsing, Information Security Manager of BankAmerica and Mr. Geoffrey Turner, Communications Security Manager, BankAmerica.

As I understand, they all don't have the same views by any means, but in order to save time, we thought we would allow each an opportunity to present a statement, which will be admitted into the record, and make general summary comments, and then be available for questions.

I will go in the order of appearance on the agenda here, Mr. Jack Simpson. Mr. Simpson, you may proceed.

STATEMENTS OF JACK SIMPSON, PRESIDENT, MEAD DATA CENTRAL, INC., ACCOMPANIED BY KENNETH ALLEN, SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS, INFORMATION INDUSTRY ASSOCIATION; CHERYL HELSING, INFORMATION SECURITY MANAGER, BANKAMERICA CORP. AND CHAIRMAN, DATA SECURITY COMMITTEE, AMERICAN BANKERS ASSOCIATION, AND GEOFFREY TURNER, COMMUNICATIONS SECURITY MANAGER, BANKAMERICA CORP.

Mr. Simpson. Thank you very much.

Mr. McCurdy. If you would pull that just a touch closer, if you can.

Mr. Simpson. All right.

I'm representing both Mead Data Central today as well as the Information Industry Association, which is a group of about 500 companies including McGraw-Hill and Dun & Bradstreet, IBM, AT&T and others.

First of all, we have a widely different opinion than what you have heard earlier today from Mr. Latham and others, because we are sort of on the bottom of the pile. We don't have the view from the top, but we see significantly more difficulties with NSDD–145 than has been spoken to. We see a lot more control of the private sector information.

We have had a number of visits. We have seen again a tightening of that control and believe that the current bill doesn't completely replace all of the issues but would form a base to let other things be delineated.

The biggest issue that I see with the current approach by the Administration is again the tremendous reach over into the private sector. All the information that we have today is unclassified, it is gathered up from newspapers and wire services and those kinds of sources, yet the definitions we see in NSDD–145 completely opens that up. We have had again visits from AFMAG implementing this.

Today's interpretation sounds very benevolent. The fact to it is that the controls are in place to have it be something altogether different. So, I think as we have had some discussion perhaps in the past few months, I think the rhetoric that we have heard has become much softer, gee, we aren't really going to enforce this, this is not a big deal, why are you all worried, it's up to somebody else, but the facts are there, that the controls are in place to have all the information in both the Federal systems as well as private systems controlled by the defense and intelligence community.

When it is all cut away, that's basically the fundamental issue.

The bill that you all are pushing forward here only handles the Federal side of that information. It doesn't deal with information classification. It doesn't deal with the private sector. I think it forms the base for having a policy that stretches out into the other two areas. That would be my summary.

Mr. McCURDY. Thank you, Mr. Simpson. Mr. Allen.

Mr. ALLEN. I have no separate statement but we do have a statement by the Association I would like inserted in the record.

Mr. McCURDY. It will be admitted. Ms. Helsing.

Ms. HELSING. I am Vice President and Deputy Director of Corporate Security, Bank of America and also the Chairman of American Bankers Association's Data Security Management Committee. I am appearing here today on behalf of the ABA, a group whose member banks constitute 95 percent of the industry's assets.

There has been a growing concern over the last 18 months or so about the Federal Government's direction in influencing private sector data security. That concern is shared not only by the financial industry but as well by other industries.

At many conferences and meetings I have attended over the last 18 months or so, this issue has emerged again and again as a topic of major concern. At issue is the impact on private sector security programs and initiatives resulting from NSDD–145.

The ABA supports H.R. 145 as a measure that will counteract the negative impact of NSDD–145 and restore a balanced relationship between the Government and private industry.

The first issue of concern is an apparent move to protect all sensitive information in basically the same manner—business information, information concerning the national interest, and classified defense information. Within both the public and private sectors, there is a need for a broad spectrum of information system security tools, techniques and standards. There must be a range of security solutions that can be matched to the value of the information being protected and to the nature of the threats.

Outside of the classified and the national security arenas, both the private and public sectors must select cost effective security controls. As a very simple analogy, consider the movement from point A to point B. In selecting a vehicle, you could select a motorcycle, a truck or a tank. All these vehicles have widely varying costs, and each is best suited to a different kind of terrain and environment.

Under NSDD–145 and the actions that have resulted from that directive, the range of computer solutions being developed have been very narrowly focused on the "tank" end of the spectrum. The danger in doing this is that the road to be traveled might not accommodate the tank, or the traveler might not be able to afford the price tag, and thus, the trip might not be taken at all.

An example of how this danger has affected the banking industry is seen in NSA's Commercial COMSEC Endorsement Program. Banks have spent several years developing a new technique for ensuring the integrity and the authenticity of electronic funds transfers and other information that we call "message authentication".

At the same time, our industry began to make significant use of encryption to protect the privacy of information stored in computers and transmitted over telecommunications facilities. Both of these techniques employ the Data Encryption Standard, more commonly known as DES, which was established by the National Bureau of Standards in 1977, and has proven to be a reliable security technique.

Following NSDD-145, the National Security Agency announced a new set of encryption algorithms under CCEP and stated its intention of discontinuing existing DES equipment endorsement programs in January 1988. The attendant publicity caused widespread belief that DES is no longer a prudent safeguard, and cast a shadow on its continued use.

Yet, after more than ten years in the public domain, no one has yet succeeded in compromising the security afforded by DES. There is no evidence that indicates DES is near the point of being broken and if there were, there are some very simple changes that can be made to the way in which we use DES that would dramatically increase the difficulty of that task.

Now, under the announced requirements surrounding the use of NSA's new CCEP algorithms, they cannot be used by our industry. The requirement simply won't work for us. Those conditions may be appropriate for national defense-related security techniques, but are clearly inappropriate for the financial industry.

This development certainly put the banks in a difficult position. Years of work and many millions of dollars devoted to encryption and message authentication efforts were jeopardized. The ABA Data Security Committee initiated dialogue with the National Security Agency beginning in October of 1985 on this issue. We reached agreement last week, I'm very happy to report, that NSA would continue to support the financial industry's use of DES-based technology until an acceptable replacement is available.

We are pleased that NSA was ultimately receptive to our needs and operational constraints, but 16 months elapsed while we worked to educate NSA about our business. Our industry has lost momentum in improving our security technology and it remains to be seen if we can overcome the damage that has been done to the perceived security of DES based techniques.

The way in which this issue arose brings us to another private sector concern with the mechanisms established by NSDD-145. The CCEP program was developed in secrecy, without any determination of the private sector's needs or constraints in using cryptographic requirements, cryptographic safeguards, and I assume that information systems security solutions are still being developed with the stated intent of having broad applicability to the private sector. Yet, there is no formal means to gather direct input about our needs or the characteristics of the business environments in which we operate.

So, one of the most important aspects of H.R. 145 from our perspective is the establishment of a formal mechanism for communication and cooperation with the Federal Government in the form of a Computer Security and Privacy Advisory Board.

One recommended change that the ABA would like to suggest would be to add a new group of representatives to that Board, to add a new paragraph in Section 19(a) to read as follows, "Four members outside of the Federal Government who are users of the technology and who have computer systems management experience, including computer systems security and privacy experience."

The ABA also supports H.R. 145 because it places responsibility for non-defense-related information systems security activities with the National Bureau of Standards, an agency with a long record of accomplishments of proven usefulness to the civil and private sectors.

Federal Information Processing Standards and special publications issued by NBS on computer security topics have been widely used and accepted as industry standards in both the public and private sectors. NBS staff have interacted openly with the civil and private sectors since the early 1970's and have exhibited an excellent understanding of the need to balance security objectives with cost effectiveness.

The rapport NBS has achieved with the financial industry in particular is partly due to the major contributions they have made in the development of our electronic funds transfers security standards. Their work on these efforts has exemplified their grasp of our need for effective yet flexible security techniques.

At the same time, we do recognize the tremendous expertise and resources resident in the National Security Agency. The NSA and NBS have worked cooperatively in the past and should continue to do so in the future.

We would recommend that this legislation include a clear statement of the relationship between these two agencies to preclude future confusion about their respective roles.

The financial industry's view of that relationship is that the National Bureau of Standards should have primary responsibility for information systems security initiatives affecting unclassified information, while the Department of Defense would have primary responsibility for information systems security initiatives affecting classified or national security-related information.

The National Security Agency should continue to serve as a technical resource to NBS, while NBS acts as the primary Federal Government liaison to the private sector. We believe the private sector would benefit from the expertise of both groups by channeling our requirements through the agency with which we have an established working relationship and a track record of successful results. This would restore the mutually beneficial and synergistic relationship that existed between the public sector and the private sector prior to the changes wrought by NSDD-145.

In conclusion, the American Bankers Association endorses H.R. 145 as a means of reversing the counterproductive impact of NSDD-145 and its resulting policy programs upon the financial industry.

Thank you for this opportunity to appear before you today.

Mr. McCurdy. Thank you, Ms. Helsing. Mr. Turner.

Mr. Turner. Thank you, Mr. Chairman.

In the interest of brevity and to avoid repetition, I'll confine my comments to the discussion that's gone before today.

The Bank of America is here in addition to the ABA today, because we feel that the issues surrounding the magic number 145 are wide ranging and go well beyond the civil sector's requirements for computer security, and in fact, have a large impact directly and indirectly on the private sector. I don't believe that this can be categorized as a simple turf war for that reason.

There are a number of ramifications that derive from this basic feature of the debate, over who should be responsible for Federal computer security policy. I agree with Mr. Walgren, that there are significant differences between the private sector, the civil sector and the defense sector on how computer security is best approached.

Referring to my colleague's reference to the tank and the motorcycle, I believe that the types of computer security programs that we find coming from the National Security Agency are very much overkill in environments such as the private sector.

In the private sector in particular, we may find that some of their solutions for securing systems designed to protect classified information are in fact too costly to implement.

On the other hand, the American National Standards Institute has several committees developing standards to protect information security in the private sector environment. This is being done with the intensive support of the National Bureau of Standards, and their contributions to this have been particularly valuable because they understand our environment in the private sector.

The solutions that we've developed from there are also being implemented in the civil sector of the Government as well. The Department of the Treasury is implementing a program to protect Federal EFT based upon the standards that were developed jointly between the private sector and the National Bureau of Standards.

I believe that the National Bureau of Standards is much more prepared, trained and ready right now to provide the type of support in the civil sector of the Government that is required to secure the sensitive information in the civil sector. I believe that the National Security Agency is not appropriate to provide this—provide the mainstream support for this effort to secure information in the civil sector and flow over in the private sector for several reasons.

Number one, as it was mentioned earlier this afternoon, the primary mission of the National Security Agency is national security. Anything else that they're required to do is going to have a lower priority than national security, and that is quite correct. The requirements of NSDD-145 that the National Security Agency cover things well beyond the scope of protecting national security are going to become more difficult to meet and are going to detract from their primary mission.

In addition, the National Security Agency, as a primarily classified national defense agency, are a closed and insular agency and are difficult to gain access to. The technology, research and development, the expertise, is all resident within the National Security Agency, but its ability to provide that and interact with nonclassified entities is not currently in existence.

I spent, as a BankAmerica representative, 18 months going through three different divisions in the National Security Agency and talking to numerous different representatives in each, without arriving at a significant dialogue. It was not until I spoke with Mr.

Daniels, the Deputy Director for Information Security, that we finally began to move toward a satisfactory dialogue.

I believe that the National Security Agency is very much unfamiliar with the computer security requirements that are particular to the private sector and to the civil sector of Government. I believe that any solutions that they try to implement will be in some parts too expensive, and in some parts too cumbersome, and may in fact impede the operation of government, and if they were to be used in the private sector, the operation of business as well.

I believe that any effort by the National Security Agency to come up to speed on its ability to interact in these environments outside of national defense would be lengthy and costly, both in dollars, and in the time lost in implementing information security in the civil and private sectors.

I believe the National Bureau of Standards is much more prepared, experienced, and is currently providing this type of support, which can readily be expanded much more easily than the National Security Agency can be trained to come up to speed.

One last comment would be that in view of my own experiences as a Naval Intelligence Officer, and 14 years experience with the intelligence community, I would look at the perspective of the National Security Agency, and if I were being put as the Director of the National Security Agency in the position of providing the protections and being responsible for the security of civil, and in some cases, private sector information, and at the same time being responsible for collecting communications intelligence, I would be very uncomfortable with that, as a National Security Agency Director, let alone as a private citizen.

Bank of America is very interested in what was discussed here today about arriving at a clear definition of responsibilities between the National Bureau of Standards and the National Security Agency, but we would be very interested in ensuring that the National Bureau of Standards has primacy in the civil side of this problem with the support on the technical research and development coming from the National Security Agency through the Bureau of Standards.

Bank of America very strongly supports H.R. 145 as a good step in the right direction, plus providing adequate and cost effective information security in the civil sector of the Government and its beneficial effects on the private sector as well.

Thank you, Mr. Chairman.

Mr. McCurdy. Thank you, Mr. Turner.

Somewhat facetiously, I guess I can ask if you'd feel differently if your father was still in charge over at the CIA but I won't even put you on the spot for that. We appreciate your testimony, and certainly appreciate your experience and your background in intelligence areas.

I guess this is to the panel, and Mr. Simpson might want to respond first. You heard the doctor, Dr. Latham, earlier, and the Department of Defense assert that it has no interest in restricting access to commercial data bases, and that the information industry has overreacted to a so-called non-issue. Do you want to comment further on that?

Mr. Simpson. I'd love to comment on that. Thank you.

Mr. **McCurdy**. I thought you might like that soft ball in the middle.

Mr. **Simpson**. I'll start by a quote that was in The Washington Post on May 27, 1986 by Assistant Secretary of Defense, Don Latham. He was quoted as saying,

> I'm very concerned about what people are doing and not just the Soviets, if that means putting a monitor on NEXUS type systems, then I'm for it. The question is, how do you do that technically without interference.

Well, he's talking about monitoring private computer systems, private information sources, and unclassified data.

When the Air Force Management Assistant Group visited us in April, five people came in. They were asking questions about who uses the system, could you put a monitor on it? How much do the Soviets use? Can this be done? Can that be done? And they were there in an implementation mode.

They wrote a report which has been classified, and none of us have been able to see it, but the actions all seem to indicate implementation and control of private sector information even though they profess not to do that. And there's several other instances, and in the interest of time, I won't do all those, but I can certainly submit those as part of the record.

Mr. **McCurdy**. Do you philosophically—do you have philosophical differences with the opinion that the Soviets could make use of certain classified and sensitive information?

Mr. **Simpson**. Yes, I do, because the whole premise of the information industry is that the information which we provide and facilitate has been classified already and that if information is unclassified in print form, it's hard for us to believe when it goes into a computer that it gets a magical transformation. What the computer may be doing is very accurately pinpointing places where classified information slipped out. It may well do that. But there isn't any magic transformation that takes unclassified stuff and makes it into something more valuable than that.

Our suggestion would be to go back and take a really close look on the classification process. We've seen some documentation from commerce that indicated that they weren't real happy with perhaps the process that DOD had used in the past about reaching their classification in terms of daily operations.

Mr. **McCurdy**. Isn't it your business though, to be seeking out so-called classified information?

Mr. **Simpson**. We don't want any classified information. We have no interest at all in that. The information we gather are things like the patents, we gather financial information from the SEC, we gather all of the information from the Supreme Courts, Attorney Generals, trial courts, and we deliver that information to law firms, we deliver it to—the Congress itself did 40,000 searches last year in various data bases that we have. The White House did 9,000.

I guess our question is, would the Congress or would the White House really want DOD going through the unclassified information before you get a chance to look at it? This is all information that is unclassified.

Ms. **Helsing**. Mr. Chairman, may I add a word to that?

Mr. McCurdy. Certainly.

Ms. Helsing. There seems to be some differences of opinion between the letter of the directive, NSDD-145, and the actions of those who are implementing that directive. We heard today that DOD and NSA believe they have no purview to come into a civil sector agency or into a private business, and direct what type of information should be considered to be sensitive yet unclassified, and thus require some type of control.

I can only conclude that the spokespeople for those agencies are unaware of some of the actions of other representatives of their agencies in dealing with the private sector. NSA personnel have come as authorized representatives to the American Bankers Association. They have told us that they consider the U.S. payment system to be a prime target of interest to an unfriendly foreign government, and therefore that information going through that payment system would be sensitive yet unclassified. We were not told that was our decision to make.

Mr. McCurdy. Thank you. The gentleman from Missouri.

Mr. Buechner. Ms. Helsing, the U.S. payment system, what do they mean by the U.S. payment system?

Ms. Helsing. Well, that was the term used by the NSA, so I hesitate to provide a definition in their terms.

Mr. Buechner. Did they give you who we pay what to?

Ms. Helsing. They were speaking about the electronic funds transfer systems of the banking industry in the United States.

Mr. Buechner. Can you tell me if you have any idea what the banking industry pays for security for its computer systems currently?

Ms. Helsing. No. I have to confess I didn't come here with the statistics on that subject. I would be pleased to provide a written response for the record.

Mr. Buechner. If you could. Does anyone here on the panel have any idea of what they—what BankAmerica is spending right now?

Ms. Helsing. Well, we are certainly talking about a very, very large investment. You can be assured that the financial industry has a great concern for computer security. Information is the lifeblood of our business. We don't have vaults full of gold and currency; we have information in computers. We fully recognize that and information security has been a top priority ever since the first computers were introduced into——

Mr. Buechner. I'm aware of that but I was looking for some cost estimates of what currently you are spending as an industry for computer security. Mr. Turner?

Mr. Turner. Sir, without providing precise figures, last year I am aware of 5 or 6 major projects within BankAmerica Corporation, the sum of which was in excess of $2 million, and that is a conservative estimate.

Mr. Buechner. Mr. Simpson, have you ever worked with either NBS or NSF on standards to secure information?

Mr. Simpson. I have not. In my previous career with the IBM Corporation, I had experience developing Tempest devices for printers and telecommunications, but in the last five years, with Mead Data Central, I've had no relationship. I wasn't connected to either of those.

Mr. BUECHNER. Mr. Allen.

Mr. ALLEN. When I was with the Government, I was with the Office of Management and Budget for 9 years. I did work with the National Bureau of Standards on standards activity, general things, policy activity.

Mr. BUECHNER. Can anybody here give me a case example where NSDD-145 has created any particular negative impact on their company?

Mr. TURNER. Absolutely, sir.

Mr. BUECHNER. Go ahead.

Mr. TURNER. Under NSDD-145, the National Security Agency felt the need to more strongly move into the area of protecting communications security in the civil and in the private sectors. This generated the so-called DES controversy. The DES controversy has very seriously impacted both my bank and the industry in several ways.

My company in particular was impacted due to the lack of confidence in DES that was engendered by the NSA's statements concerning the lifetime of DES was going to expire in 1988, they had something bigger and better called CCEP.

This had the effect of discouraging vendors from making the investments to develop the technology that we need to implement DES technology to protect EFT and other types of sensitive information in our bank right now. We are ready to implement right now. We want the technology right now, and the NSA was discouraging the development of vendors to create the technology to support that. This is also causing a lot of the other institutions, not only banking, but in other industries as well, from going ahead and contacting the vendors and saying, we would like to have security products, using DES to protect our information.

So I felt that it very much slowed down implementation of information security, particularly using encryption, by the actions that the NSA took in response to what they saw as their mandate under 145.

Mr. SIMPSON. I have another case. On February 17th, we removed from our system, the NTIS files, all of the Department of Energy information and so forth, that we were delivering to many customers. We did it for a combination of reasons. It was a borderline economic situation, and we figured that it was not worth the grief to continue with it. We wanted to sharpen the point that that was surely the only thing that could possibly be in question. So by removing that we would not expect to have any other issues out of NSDD-145. So that remains to be seen. But some of our customers are upset that they can no longer get the NTIS file.

I would like to make one other point if I could. We have a lot of difference of opinion about what security means. Security to us who make a living out of delivering electronic information means maintaining the privacy among our users about what they do. A large law firm, or the Congress, or the Senate, does not want to have someone be able to monitor what they're searching, because you can understand the people you're looking at, you can understand the train of thought, and yet Mr. Latham today in his testimony indicated that that's the kind of thing they're interested in. They want to see what the Soviets are looking at, or maybe this marginal company that might deal with the Soviets. Who would make that decision? How far does it go? Would everything be looked at? Who decides what's going to get monitored?

So, security to us means being able to have people use these computer tools, scientists, researchers, business, judges, without concern for who is looking at their information. Yet security in many other senses is hardening the system and not letting someone pick up that information. So security depends really on what point of view, who are you trying to protect.

Monitoring a system to see if Soviets are using it, is in fact invading the privacy of those people that might use the system.

If our users thought that you could monitor their research results, then this whole industry is all over with, and our intent is not to do that. We don't want such monitoring. So it's a Catch 22.

Mr. BUECHNER. Thank you, Mr. Chairman.

Mr. MCCURDY. Thank you, Mr. Buechner. I would just like to say how clear the testimony is, certainly what both Ms. Helsing and Mr. Turner have given us to this DES circumstance, and it is certainly striking, and particularly, it deserves to be underscored, the point you make that this more secure system that undercut the use of DES and the development of DES was developed without any contact with the private sector at all. And that as you say clearly in your testimony, and I say just to underscore it, that the Committee which develops the operating policies necessary for implementation of NSDD-145 does not have a single private sector representative, despite the intent of applying results of that directive to the private sector. To me, that's very telling, and I appreciate the clarity of your testimony. It's very strong.

With that, the gentleman from Iowa. No—Missouri.

Mr. BUECHNER. It's Missouri. It's real close sir, don't worry. There's a gentleman from Missouri who spends a lot of time in Iowa, I think that may have you confused on that. [Laughter.]

Mr. MCCURDY. I was just in Missouri and Iowa, and——

Mr. BUECHNER. You know how to frequent fly? [Laughter.]

Mr. Simpson, as a follow up, as we go through this interchange, it's pretty obvious that everyone is concerned about security and sensitivity, but do you have any suggestions that you can make on how to protect both military and civilian data bases?

Mr. SIMPSON. I think the solution has to be more clearly defining what we're talking about, because I think you've got the military data bases, you've got civilian, federal, you've got private. And when you apply a rule, let's say of sensitive and unclassified to take care of payroll, and internal information in the Federal sector, to take that rule and drop it into private, it says that all unclassified is opened up again. I think we're trying to solve several problems with one grand closed form rule.

Mr. BUECHNER. Would you acknowledge that there is a problem?

Mr. SIMPSON. I would say this in the private sector, that our whole business has been built upon the classification system today working. I think that the classification system today was done without knowledge of computers. Therefore, things that are classified, small ones may have slipped into the system, so I think you have to go back and re-evaluate whether that is working properly or not.

But to my knowledge, everything that the industry, in the private sense has, is unclassified, and we don't believe we're adding to the problem.

The problem with internal data inside civilian federal computing systems probably is there. It's just that when you are solving this, which seems to be the main intent of NSDD-145, the rules that are being applied there, when they come over into the private sector, create great difficulty for us. And I think we have a mentality that only understands this world; we don't see the other world very well. We don't seem to interchange very well.

Mr. BUECHNER. All right. I'm going to ask you to do the same thing I asked of the previous panel.

Mr. SIMPSON. All right.

Mr. BUECHNER. And that is, if you've got any definitions or any suggestions, we would appreciate receiving those in writing. I mean, if you can come up with a definition of "sensitive," if you can draw the line, then I think we'd appreciate your input, just as we have from the previous testimony.

Mr. SIMPSON. Thank you. We will give you an input on that.

Mr. ALLEN. Mr. Congressman, I might note that there is a definition of "sensitive" already in current government policy. OMB has a computer security policy now, A-130, Appendix 3, I believe it is, that has a definition of "sensitive information" in it; it has had for three or four years, when it used to be something called OMB Policy A-71.

The definition, as I recall, does not encompass everything in the world as the NTISSC No. 2 does, but says that agency heads should assess the risk of loss associated with data by doing risk analyses, and then should implement standards commensurate with whatever that risk is.

That is current policy. It seems to be adequate. It's not clear that there is a need for additional policy in this area. Working closely, using that policy and the current NBS standards, it would seem sufficient authorities, as well as the law, such as the IRS Code and the Census Code and all, which require protection of information, such that we do not need an NSDD-145. The authority and the requirements already exist, as far as the Government is concerned.

Mr. WALGREN. Thank you, Mr. Buechner.

Let me try to understand, at this point, assuming a bill like H.R. 145 would pass, the Government may still come in and do something, promulgate a standard that is different from the DES standard, but you would essentially be dealing with a National Bureau of Standards that was in consultation with the National Security Agency, instead of dealing directly with the National Security Agency.

And as I understand it, you now use—the obvious tradition in the National Bureau of Standards of taking account of the private sector and private sector needs that you found almost totally lacking when you dealt with the National Security Agency directly; is that correct?

Mr. SIMPSON. That's a very good summary, Mr. Chairman.

Mr. **Walgren**. Well, let me, on behalf of the committee, thank you all for your testimony, and we appreciate the contribution that you've made to our process here. Thank you very much.

[The prepared statements of Mr. Simpson, Ms. Helsing and Mr. Turner follow:]

Information Industry Association
555 New Jersey Avenue, N.W., Suite 800
Washington, D.C. 20001
202/639-8262
Cable: INFORMASSN WASHINGTON

Testimony
of
Jack W. Simpson
of
Mead Data Central, Inc.
on behalf of the

INFORMATION INDUSTRY ASSOCIATION

Before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
SUBCOMMITTEE ON SCIENCE, RESEARCH, AND TECHNOLOGY
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS

on

H.R. 145

February 26, 1987

FOR RELEASE ON DELIVERY EXPECTED ON THURSDAY, FEBRUARY 26, 1987

STATEMENT OF JACK W. SIMPSON
PRESIDENT OF MEAD DATA CENTRAL, INC., DAYTON, OHIO
BEFORE THE COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
OF THE
UNITED STATES HOUSE OF REPRESENTATIVES

Mr. Chairman and members of the Committee. I am Jack Simpson, President of Mead Data Central, Inc. of Dayton, Ohio. For the record, I would like to note that I appear on behalf of Mead Data Central as well as the Information Industry Association. With me today is Ken Allen, Senior Vice President of the Information Industry Association. This association represents almost 500 of the leading information companies such as Mead Data Central, Dow Jones, Dun and Bradstreet, McGraw-Hill, the Washington Post and IBM in the United States and around the world.

I appreciate this opportunity to appear before the Committee to discuss H.R. 145, "the Computer Security Act of 1987", and related issues. I would like to preface my comments on the bill with a brief explanation of the information industry and Mead Data Central, Inc.'s part in that industry.

It has been widely recognized that we are on the dawn of a new era, an information age in which the information industry will become as important as the old smokestack industries were in their era. A 1980 study for the Department of Commerce concluded that the information sector of our economy constituted 34% of the gross national product and 41% of the nation's labor force. One of the fastest growing sectors of the information industry is the online database industry of which Mead Data Central is a leading player. In 1979 there were 221 worldwide database producers and 400 online databases. By 1986 there were almost 1500 database producers and 3200 databases. A growth of 8 times. The number of online services through which such databases are available grew from 59 to 486 during the same period. In 1984 an Office of Technology Assessment study estimated that the online information industry generated $3.65 billion in revenues. The United States is the leading provider of online services: 18 of the 20 largest international online database companies are American. Better than a billion dollar trade surplus is generated by this young industry.

Mead Data Central, Inc. markets computer-assisted information retrieval services worldwide for use by corporations, news media, government and the legal, medical and accounting professions. MDC is a Dayton, Ohio company and began operations in 1972, which makes it one of the oldest companies in the industry. MDC's databases are among the largest private sector collections of electronic information in the world, and contain 47 million full-text documents, comprised of 137 billion characters. These documents come from a wide range of sources, such as newspapers, magazines and federal, state and local governments.

MDC's information databases are arranged into subject categories we call Services. These include LEXIS^R, a computer-assisted legal research service; NEXIS^R, a computer-assisted news, business, marketing and general information retrieval service; EXCHANGE^{TM}, a financial information service; MEDIS^{TM}, a medical information service of clinical journals and reference databases; LEXPAT^R, a full-text database of U.S. patents since 1975; the National Automated Accounting Research System (NAARS), a database of annual reports and proxy information produced in cooperation with the American Institute of Certified Public Accountants; The Reference Service (REFSRV^{TM}), a compilation of bibliographic abstracts and other reference databases; and LEXTRACK^{TM}, which provides private litigation support libraries. The information in these databases is distributed to subscribers via MDC's custom terminals as well as personal computer equipment supplied by other vendors.

Micromedex, Inc., a wholly-owned subsidiary of Mead Data Central, Inc., markets medical databases, including Poisindex^R, a database which recommends treatments for poison consumption. Micromedex markets its databases on microfiche and through compact disc technology.

The documents in MDC's Services and those of the other companies making up the Information Industry Association have one thing in common: they are composed of publicly available, previously published, non-classified information.

The emerging information age is beginning to bring us unprecedented access to useful information, and with it new and exciting opportunities for individual, economic and political growth. It also raises new challenges. One of these before us today is the protection of information against unauthorized use of information. This is the issue addressed by H.R. 145.

The Information Industry applauds the intent and direction of this Bill.

I believe that it is successful in establishing the appropriate minimum standards and training to ensure that the best technology and practices are applied to federal computer systems and that these standards are both appropriate and sensible.

The composition of the advisory board also appears balanced and should ensure that issues are examined from all pertinent vantage points by experienced experts.

It also seems clear that the scope of the Bill is intended to cover all federal computer systems whether operated by government or civilian organizations. Private computer systems, that is, those not operated by or for the government are not covered by this bill and therefore would be expected to only handle unclassified information.

I further note that the focus of the Bill is on the protection of computer systems and not on the classification of the information flowing in such systems. The processes for deciding the appropriate classification for government or government-derived informa~~tion ar~~e unchanged by this bill.

I submit that a clear distinction should be made between Federal and Private computer systems and a clear distinction should also be made between the control of computer systems per se and the control of information itself.

The basic premise that we in the private sector operate upon is that commonly available government information has been screened and classified and that private sector information can and in fact should be freely distributed.

Even though our private sector computer systems contain non-classified information, all of us in the industry are concerned about security. The idea of assistance to us in this area as mentioned in H.R. 145 creates no concern and is in fact welcome. Our delivery systems are built to ensure the privacy and secrecy of our clients and their search requests. We use all the customary security measures typically employed in the private sector to maintain this security.

It is appropriate, however, to draw attention to National Security Decision Directive 145 to contrast the approach taken by this document, which we feel is headed in the wrong direction.

NSDD 145 is in conflict with H.R. 145 and contains language which suggests that we in the private sector may get "help" whether we want it or not.

"In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures."

As events unfolded since NSDD 145 was issued, I began to get some insight as to how the military might apply this national security test in providing assistance.

The Department of Defense report of September, 1985, titled Soviet Acquisition of Militarily Significant Western Technology: An Update suggested "keeping sensitive information out of the public data bases" as an alternative to accomplish its goals. Rather than securing or "hardening the system" to allow the information to be protected while still flowing freely, the focus quickly moved to stripping information out by restructuring the information flow.

Of equal importance in terms of an indication of direction that could be taken was the September 29, 1986 list circulated by Walter Heiland of NASA, which identified some 33 companies who were not to be entitled to see otherwise public, non-classified NASA documents. The companies on this list were there for listed reasons such as "Canadian office in U.S.A." and "technical information collection office for Israel." They were not given notice that their rights to know were being cancelled, and in fact when the author of the list was asked about its existence by the press, he denied it. When confronted with a copy and asked why he had denied its existence, he was quoted in the January 9, 1987 Bureau of National Affairs, Daily Report for Executives, as saying that the document was "clearly indicated for internal use and therefore there is no 'No No' list." Did NSDD 145 create the atmosphere for this type of information control? Where does this end? Consider the effect that 5 or 10 years under this type of philosophy would have on the development and availability of information and technology.

The emerging direction being followed in implementing NSDD 145 is one of controls on private computer systems, controls on all unclassified information and an extremely broad "hunting license" for virtually any "sensitive information" useful in any way to an adversary even though such information has traditionally been in public hands. Such new restrictive and unwarranted policies under the unilateral control of the Defense Community threaten to bring this industry to a halt and would negate the significant productivity gains being made in many sectors of our economy including legal, financial, government, medical, and the scientific and technical community. The proposed Bill, H.R. 145 would move us in a sounder direction and provide for a balance of considerations when controlling information and computer systems that is lacking in NSDD 145.

The desire for total control of Federal and Private Computing Systems and all information they contain may be occurring because of an unwarranted fear of new technology. A basic concept contained in NSDD 145 suggests that otherwise non-classified information can become classified when enough of it is viewed in the aggregate. This is simply a fear that computers and information databases will be useful to enemies to gather up bits or classified data that may be more difficult to track in print form. It ignores the fact that computers are extremely useful to this nation when the scientific community has good access to these tools. Progress should not be stopped simply because there are some negatives. There usually are. We must weigh both the negatives and the positives and decide accordingly.

Control of civilian information processes by military and intelligence personnel applying such policies to the private sector will create a number of problems. For example.

-- A national suspicion of super secret agencies such as the National Security Agency will work against an easy, cooperative relationship with the private sector.

-- Inadequate consideration will be given to the loss of research and development that will cease to occur because information that might have triggered ideas was suppressed.

-- The philosophy being followed by the military and intelligence group, sometimes called the aggregate or mosaic theory, (i.e. even though individual bits of information in themselves are unclassified, when a large number of them are collected in one place, they may reveal classified information) is an unworkable test. Since enough of almost any information could lead to something, there is no practical way to draw a line on when and where to stop the suppression of information.

-- The benefits to the nation of a strong information industry--an industry in which the U.S. currently leads the world, approaching over a billion dollar trade surplus, would be threatened and possibly destroyed because its only inventory, information, would be subject to over-control. Development of the sciences cannot occur in the climate fostered by NSDD 145. If civilian information and technology are permitted to exist and grow only if they cannot possibly benefit potential adversaries, they can never benefit this nation either, and the loss to us will be much greater. This nation, not the Soviets, will be the loser.

I believe the very reason our system works better than that of the Soviets is because of the bias toward the free flow of information.

H.R. 145 makes great strides forward in correcting the inappropriate direction of NSDD 145, and restoring civilian control over civilian matters.

On behalf of Mead Data Central and the Information Industry Association I support H.R. 145 which provides the fundamental direction for a properly balanced computer and information security policy. I further recommend hearings be conducted on the control of information particularly in the Private Sector.

COMM06/DSPW.801

INFORMATION INDUSTRY ASSOCIATION
MEMBER COMPANIES

February 4, 1987

ABC-CLIO
ABC International (Reed Telecomputing)
Academic Press, Inc. (Harcourt Brace Jovanovich)
Access Publishing Company
Accurate Information Service
Addison-Wesley Information Services
Admax, Inc.
Advanced System Design, Inc.
Advanced Technologies Division (U S WEST)
Aerospace Online (Murdoch Magazines)
Agenda Technology
AgriData Network (AgriData Resources)
The Alexandria Institute
Amerestate, Inc. (Ohio Real Estate)
AMERICAN BANKER/BOND BUYER (International Thomson)
AMERICAN CONNECTION, INC.
American Corporate Services
American Stock Exchange Market Data Communications
American Telephone & Telegraph Company ("AT&T")
Amidon/Litman Associates
AMTEC Information Services, Inc.
Apple Information Services
Applied Information Services Inc.
Applied Information Technologies Research Center ("AITRC")
Arcata Electronic Information Services
Arthur Andersen & Co.
ASEC International, Inc.
Aspen Systems (Wolters Samson)
Associated Information Services Corporation
The Associated Press New Media MarketingGroup
AutEx Systems Inc. (International Thomson)

Baseline
base-line SYSTEMS corp.
Bechtel Information Services
Beckerman Associates
BellSouth Advertising & Publishing
BellSouth Enterprises
BellSouth Services
Berul Associates, Ltd.
THE BERWICK GROUP
BetaWest Properties (U S WEST)
BioSciences Information Service
BNA Communications Inc.
BNA International Inc.
The Bond System
Bonneville Telecommunications Company
R.R. Bowker Company
Bowne & Co., Inc.
Brattle Research Corporation
Broadview Associates
Broker Power Inc.
Alex. Brown & Sons, Incorporated
BRS Information Technologies
Buraff Publications, Inc. (BNA)
The Bureau of National Affairs, Inc.
Ed Burnett Consultants, Inc.
Christopher Burns, Inc.
Business International Electronic Services
Business Research Corporation
Business/Technology Ventures

California Information Company
Call-It Co.
Cambridge Research Institute
Cambridge Scientific Abstracts (Disclosure)
DANIEL CARTER CONSULTING
C.A.S. COMSEARCH
CCX Direct Marketing Network
Center for Birth Defects Information Services, Inc.
Chase Global Electronic Banking
Chemical Journals Online
Chicago Board of Trade Information Systems and Telecommunications Group
Citibank Global Report
Citicorp Information Business
Citicorp Information Center
Citicorp Development Division
Citicorp Electronic Securities Services
C.ITOH Communication Systems Inc.
CMQ Communications Inc.
CNR Partners
Thom Collins Consulting
Commerce Clearing House Product Systems
The Communication Studio
Compu-Mark U.S.
Compustore online
Computer Business
Computer Science Capital Corporation
COMSAT General
Conference Board Data Base

Congressional Information Service, Inc. (Elsevier)
Cooper Heller Research
Coopers & Lybrand
Corporate Management & Marketing Consultants, Inc.
Corporate Technology Information Services, Inc.
COVIDEA
Cowles Information Services
Cuadra Associates, Inc.
C W Communications

D&B Computing Services, Inc.
DAFSA KOMPASS
Damar Corporation
D.A.T.A., Inc.
Data Courier (Bell & Howell)
Data Resources, Inc. (McGraw-Hill)
Data Retrieval Corporation
Database Development
Database Services, Inc.
DataCraft, Inc.
Dataline, Inc.
DATALINE DADOS INTERNATIONAIS LTDA.
Datalogics Inc.
Datapress Inc.
Datapro Research Corporation (McGraw-Hill)
Dataquest (D&B)
Datasolve Database Information Service
Datatek Corporation
DATEXT, INC.
Derwent Inc.(International Thomson)
DIALOG Information Services, Inc.
Digital Equipment Corporation
Digital Information Group
Disclosure Information Group
Donnelley Information Publishing (D&B)
Donnelley Marketing Information Services (D&B)
Dow Jones & Company Inc.
Dow Jones & Company, Inc. - Information Services Division
Dun & Bradstreet Canada
The Dun & Bradstreet Corporation
Dun & Bradstreet Commercial Collections
Dun & Bradstreet Credit Services
Dun & Bradstreet Information Resources
Dun & Bradstreet Information Systems
Dun & Bradstreet International
Dun's Marketing Services
DunsNet
Duston Associates
Dynamic Information Corporation

EasyLink (Western Union)
EDS Electronic Publishing Systems
EIC/Intelligence, Inc.
Electronic Information Systems
Electronic Publishing Company, Inc.
Electronistore Services, Inc. (R.R. Donnelley)
Equatorial Communication Services
Ergosyst Associates, Inc. Information Resource Center
Executive Telecom System, Inc. (BNA)
Exxon Research and Engineering Company

F.B.R. Data Base Inc.
FEICO (McGraw-Hill)
FiberLan, Inc. (Bell South)
Fidelity Investments
Financial Post Investment Databank
FINANCIAL SATELLITE CORPORATION
FIND/SVP
FINIS: Financial Industry Information Service (Bank Marketing Association)
FirsTel Information Systems, Inc. (U S WEST)
Focus Enterprise Group
Focus Research Systems (D&B)
Foursquare Software Corporation
Claire G. Fox
FROST & SULLIVAN, INC.
FUINCA
Fulcrum Technologies Inc.
Future Computing Incorporated (McGraw-Hill)
Future Systems, Inc.

Gale Research Company (International Thomson)
Gannett New Media Services
Garvin Information Services
Genix Corporation
Alfred M. Goodloe Associates, Inc.
Edward J. Gottsman
Goulston & Storrs (Route 128)
Gregg Corporation
Grolier Electronic Publishing, Inc.
Group L Corporation

Halcyon Associates
Hambrecht & Quist, Inc.
Handy Associates Information Division
Christopher Hegarty & Co.
Ronald L. Henderson Associates
Hill-Fay Associates, Inc.
HORIZONS Associates

Howard-Sloan Communications Search, Inc.
Huntley, MacAllister & Associates
HUTTONLINE

IBM Corporation
ICC Information Group Ltd.
IDA Ireland
I.E. Associates, Inc.
IMS INTERNATIONAL DATABASE SERVICES GROUP
iNET 2000
Info Globe (International Thomson)
Infomart
Information America, Inc.
Information Consultants Inc. (BNA)
Information Consulting
Information Dimensions, Inc.
Information Market Indicators, Inc.
Information Interface Investments
INFORMATION ON DEMAND, INC. (Pergamon)
Information Sources, Inc.
Information Systems Marketing Company
Information Workstation Group
InfoProbe Incorporated
InfoTech
Inmagic Inc (Warner-Eddison)
Institute for Scientific Information ^{R} ("ISI"^{R})
INSTINET CORPORATION
Interline Communications Services, Inc. (U S WEST)
International Data Corporation
International Development Center
International Thomson Library Services
Manley R. Irwin
Item Data Incorporated

Jamaica National Investment Promotion
J.L. Joslin Associates, Inc.
The Journal of Commerce (Knight-Ridder)

Kadec Information Management Company
Kapor Enterprises
Marlyn Kemper
KEYCOM Electronic Publishing
The Kilty Company
Kirkland & Ellis
KLUWER
Knight-Ridder Business Information Services
Knight-Ridder Commodity New Services, Inc.
Knight-Ridder Money Center
Knight-Ridder Tradecenter
Kyodo News International, Inc.

Landmark Publishing Company(US WEST)
Langley Publications, Inc.
LaserData, Inc.
Laser Resources, Inc.
Lawler Associates
Leading National Advertisers
Learned Information, Inc.
Legi-Slate (Washington Post)
LifeCard International
LIGHT Magazine
LINK Resources Corp. (International Data Corporation)
Arthur D. Little Information Industry Practice
Lloyd's Maritime Data Network (Mardata)
LOGIN Service - Control Data
Lotus Development Corporation Information Services Division

Mainstream Data
Donald Marchand
Market News Service, Inc.
Mayers & Associates
McGraw-Hill Book Company
McGraw-Hill Broadcasting Co., Inc.
McGraw-Hill, Inc.
McGraw-Hill Information Systems Company
McGraw-Hill International Book Company
McGraw-Hill Publications Company
McKinsey & Company, Inc.
McPherson's America Inc.
Mead Data Central
Media General, Inc.
Medical Economics Company (Internat'l Thom.)
Meredith Diversified Company
Meyers, Tersigni, Kaufman, Lurie, Feldman & Gray
Micromedia Limited
Microsoft CD ROM Division
Monchik-Weber (McGraw-Hill)
Monosson Technology Enterprises
Moody's Investors Service (D&B)
Moore Data Database Publishing Group
Morgan Rand Publications, Inc.
The Morris Group for Information Technology
Mountain Bell (U S WEST)
MULTICOMM Telecommunications Corp.
MULTIPOINT COMMUNICATIONS LTD.(Bonneville)

National Computer Network Corp.
National Decision Systems
National Planning Data Corporation
National Satellite Paging, Inc.

Neodata Services (D&B)
NERAC, Inc.
Nevada Bell (Pacific Telesis)
New York Futures Exchange, Inc.
New York Stock Exchange, Inc.
New York Pulse
NewsBank Inc.
Newsday Videotex Services (Times Mirror)
NewsNet Inc.
Newsweek (Washington Post Co.)
Nielsen Clearing House (D&B)
Nielsen Marketing Research (D&B)
Nielsen Media Research (D&B)
Northwestern Bell (U S WEST)
Novatron Information Corporation
NYNEX Corporation

Occupational Health Services, Inc.
Official Airline Guides (D&B)
Offshore Information Services Inc.
Ogilvy & Mather Videotex Development Group
Online Access Publishing Group
Online Computer Systems, Inc.
Online Connection, Inc.
ORI, Inc. Information Systems Program Office
The Oryx Press

Pacific Bell
Pacific Bell Directory(Pacific Telesis)
Pacific Data Services, Inc.
Pacific Telesis Group
Pacific Telesis International
Packard Press-Washington
PacTel Corporation (Pacific Telisis)
PacTel Directory (Pacific Telesis)
PacTel Infosystems (Pacific Telisis)
Paget Properties, Inc.
PaineWebber, Inc.
Panel Publishers, Inc. (Wolters Samson)
Pasha Publications Conference & Book Division
PEAT MARWICK
Peeke LoanFax, Inc.
Pergamon InfoLine, Inc.
Petroleum Information (D&B)
Pharmaco-Medical Documentation, Inc.
Philips and Du Pont Optical Business Company
Philips Subsystems and Peripherals, Inc.
Phillips Publishing Inc. -- Publications Group
Phone Programs, Inc.
Pike & Fischer, Inc. (BNA)
PLASPEC
The Pofcher Company
Richard Pollard
Port Import/Export Reporting Service (Journal of Commerce) ("PIERS")
Post-Newsweek Stations (Washington Post)
Predicasts (ITG)
Prentice-Hall Information Services
PRIVATE SATELLITE NETWORK, INC.
PRN Associates
Projections Company
PsycINFO
Publishers Data Service Corporation

QUANTUM Computer Services, Inc.
Quest International
Questel, Inc.
Quick & Reilly, Inc.
Quotron Systems, Inc. (Citibank Information Business)

Rand McNally - Infomap, Inc.
Random Corporation
READEX Microprint Corporation (NewsBank)
Real Decisions Corporation
Reed Telepublishing, N.A.
Reference Technology Inc.
The Researcher's Data Bank
Research One
Research Publications (International Thomson)
Reteaco Inc.
Reynolds & Reynolds Interactive Solutions
RFP, Inc.
L. Michael Ridder, Inc.
Joseph M. Ripley
Rowe Software
Russell Associates

Saztec International
Schwab Investor Information Service
SEC Online
Selected Information Retrieval Company Inc.
SENCOR
I.P. SHARP ASSOCIATES LIMITED
Shepards (McGraw-Hill)
R. Shriver Associates
SilverPlatter, Inc.
Charles E. Simon and Company
SNET Communiaation Services
SNET Directory Operations
Sociological Abstracts, Inc.
Solution Associates
SONY Optical Memory Group

Source Telecomputing Corporation
South Central Bell (BellSouth)
Southern Bell (BellSouth)
Southern New England Telephone ("SNET")
Southern Satellite Systems/Tempo Data
Southwestern Bell Corporation
Southwestern Bell Mobile Systems, Inc.
Southwestern Bell Publications, Inc.
Southwestern Bell Telecommunications, Inc.
Southwestern Bell Telephone Company
SPUR (San Francisco Planning and Urban Research)
Standard & Poor's Corporation (McGraw-Hill)
Starcom International, Inc.
States News Service
Stigelman Associates, Inc.
Straat Group Incorporated
Strategic Intelligence Systems
Syntactic Analyzer, Inc.

Tacheron Associates
Targeted Information Service
Tax Management, Inc. (BNA)
TECHWORLD
Telaction (J.C. Penney Videotex Services)
Telebase Systems, Inc.
Telekurs AG Financial Information Division
Telenet Communications Network Applications & Terminals
Telerate Systems Inc.
Texas Instruments Terminal Products Customer Center
Textbase Associates
Thomas Register of American Manufacturers
Tijl Datapress b.v.
Time Inc. - Magazine Group
TIMEINFORM Inc.
Time-Sensitive Delivery Guide, Inc. (Pitney Bowes)
Times Mirror Videotex Services, Inc.
TMS Inc.
TORSTAR New Business Development Group
Touche Ross & Co.
TRAC (Trend Response & Analysis Company)
Track Data Corporation
Transactions Marketing, Inc.
Transdata (American Banker)
Transworld Systems-Eastern Region
Travelmation Corporation
TRI-CO (U S WEST)
Trinet, Inc.
TRINTEX (IBM/Sears)
TriStar Publishing

TRI-TECH Data Solutions, Inc.
TRW
TRW Information Systems Group

United Communications Computer Services Group
United States Satellite Broadcasting Company, Inc.
University Microfilms International (Bell & Howell)
Unz & Co.
UPDATA Publications, Inc.
U S WEST Corporate Communications
U S WEST Direct
U S WEST Financial Services
U S WEST
U S WEST Information Systems
U S WEST Knowledge Engineering, Inc.
U S WEST Materiel Resources
Utlas, Inc. (International Thomson)

Johan Van Halm & Associates
Venture Acceleration
Venture Strategies
Veronis, Suhler & Associates Inc.
Videodial, Inc.
VideoLog Communications
Visual Information Systems Inc.
VNU Amvest, Inc.
VORTECH DATA, INC.
VU/TEXT Information Services (Knight-Ridder)

Wall Street On-Line Publishing Co., Inc.
R. TAYLOR WALSH
WANG Financial Information Services Corp.
WARNDEX Corp.
The Washington Post
The Washington Post Company
Welsh, Carson, Anderson & Stowe
West Professional Services
Westinghouse Electric Corporation
WESTLAW
Whelan Associates
John Wiley & Sons, Inc.
Wilson & McLane, Inc.
Ann L. Winblad Consultants
WindBooks, Inc.
Wright Database Services

X*Press Information Services

Zapodel Inc.

NASA Scientific and Technical Information Facility
Operated by RMS Associates

Post Office Box 8757, Baltimore-Washington International Airport, Maryland 21240 • (301) [illegible]

September 29, 1986

SEP 30 1986

TO: All TU Officers, IAC Directors And Other Members Of The TU Family

SUBJECT: The So-called "No-No List"

Attached for your information is an update of the "No-No List". As a matter of clarification, I'd like to inform you in more detail about this listing.

Since the services and documents outlined in the NASA TU Program are not available to requesters outside the United States or their in-country representatives, we have for many years screened all requests for subscription to NASA Tech Briefs and Technical Support Packages. This resulted in the establishment of the attached listing. The majority of the organizations listed cater to information requests from both, the national and international arena. Due to this fact and in accordance with NASA policy we have rejected in writing their subscription or document requests with the understanding that we would mail information directly to their client if the address is provided to us. We feel that in this manner we circumvent potential problems of American requesters using the services of the businesses on the attached listing.

If you have any questions don't hesitate to call us. We will provide an update on a regular basis as we add additional organizations.

Sincerely,

Walt Heiland

Walter M. Heiland
Manager, Technology
Utilization Office

LIST OF ORGANIZATIONS NOT PROVIDED WITH SUBSCRIPTION TO NASA TECH BRIEFS, TECHNICAL SUPPORT PACKAGES, OR OTHER TU DOCUMENTATI

Name/Organization	Location	Remarks
British Aerospace	Virginia	
C Itoh & Co., (America)	335 Madison Avenue, NY	Japanese Company
Caleb International		
Coordination Council For North American Affairs (CCNAA)	Washington, DC	Republic of China
ERSO/ITRI	Santa Clara, CA	Republic of China
Find-SVP	500th Avenue New York, NY	French Info. Colle ion Agency
Fujitsu Microsystems of American	San Jose, CA	Japanese Informati Collection Agency
Geosat Committee, Inc.	San Francisco, CA	International Distribution of Technical Information
Heraeus Volkert, Inc.	Queens Village, NY	Worldwide Dissemination of Info.
Info Doc	Dulles Airport, DC	Worldwide Dissemination of Info.
INFO/CONSULT or Teldan (Ms. G. Revesz)	P.O. Box 204 Bala Cynwyd, PA	Major Supplier of Technical Information to Israel
Information on Demand	Berkley, CA	International Distribution of Technical Information
Instruments SA, Inc.	New Jersey	South American Company - Rep. Office
Intercon Research Associates, Ltd., (Sigrid Pilgrim)	Evanston, IL	International Supplier of Technical Information
International Research & Evaluation (IRE) - (Dr. King or Dr. Danford)	Eagan or Bloomington, MN	Possible International Distribution of Documents

Name/Organization	Location	Remarks
Islabor Co.	New York	
Israel Aircraft Industries, Inc. (IAI or ELTA)	50 W. 23rd Street, NY	Technical Information Collection Office For Israel
Jet Int'l gr	P.O. Box 020010	International Supp
Jet Cargo Int'l	Miami, FL 33102	of Tech Info.
JNIP - Jamaica National Investment Promotion Ltd.	Hayward, CA	International Technology Transfer
JSR America, Inc.	5th Avenue, NY	International Distribution of Technical Information
Kitao Publications Trading Company	Forest Hill, NY	International Supplier of Tech. Inf
Olympus Management, Canada	Hollywood Hills, CA	Canadian Office in USA
Parker Comm. Co., Ltd.	Michigan	International Technology Transfer
Dr. Michael Radner -- Northwestern University	Evanston, IL	Involved in Hi-Tec Transfer With Japanese Firms
RPA Subscription Agency	Miami, FL	South-American Collection Agency
Romar Enterprises	Lake Tahoe, CA	Dissemination of Technical Information Worldwide
Scitex or Scitek America Corp.	New York	
Seaboy Marine Services		
Toyota Motor Corp. (Rep. Office)	Washington, DC	Japanese Representative in USA
United Book Services	7th Avenue, NY	International Supplier of Tech. Inf
University Microfilm International	Ann Arbor, MI 48106	International Distribution of Technical Information
Washington Bibliographic Service, (Alan Seltzer)	Silver Springs, MD	Dissemination of Technical Information Worldwide

Name/Organization	Location	Remarks
Zoom International Courier	Miami, FL	South-American Collection Agency

ALL EMBASSIES AND CONSULATES IN THE USA, AND REPRESENTATIVES OF FOREIGN COMPANIES OR ORGANIZATIONS ARE TO BE INCLUDED ON THIS LIST

NASA RESTRICTS ACCESS BY FOREIGNERS TO TECHNICAL INFORMATION AVAILABLE IN LIBRARIES

The National Aeronautics and Space Administration has long restricted access by foreign companies or their agents to unclassified technical materials, a policy criticized by the Information Industries Association.

This longstanding NASA policy has resulted in preparation of an internal "no-no list" of 33 persons or companies banned from receiving a publication called "NASA Tech Briefs," a summary of engineering information based on NASA projects.

The list of 33 entries begins with British Aerospace, Inc., includes Toyota Motor Corp., and ends with Zoom International Courier. About one-third of the companies on the list are U.S. firms specializing in information retrieval, including University Microfilm International, of Ann Arbor, Mich., and RPA Subscription Agency, of Miami, which the list describes as a "South American collection agency."

NASA Official Denies Existence of "No-No List"

"There isn't such a list," according to Walter Heiland, manager of the Technology Utilization Office. However, Heiland's signature is on a Sept. 29 memo that begins, "Attached for your information is an update of the 'No-No-list.' "

"That document was clearly indicated for internal use, therefore, there is no 'no-no list,' " according to Heiland, who said the list is now slightly smaller and is no longer called the "no-no list."

Heiland said the list reflects a decade-old NASA policy which states, "Documents and services from the NASA technology utilization program are not available to requesters outside of the U.S., or their in-country representatives."

Heiland said, "That's nothing new, that is and has been NASA's policy." He could not cite the legal authority for the list, but a NASA legal expert explained that it derives from a section of the 1958 Space Act which says NASA should "provide for the widest practical and appropriate dissemination of information concerning its activities and the results thereof."

As Heiland puts it, "Your and my tax money has paid for the technology and therefore it should be available to American engineers first." The reason for the development of the bimonthly "NASA Tech Briefs" is to give the American engineers the first crack at new technologies, according to Heiland. The material is all unclassified, and publicly available for free. Also free from NASA, but again only to U.S. citizens and companies, are "Technical Support Packages," which provide far more detailed information about subjects covered in the "Tech Briefs," and also are unclassified.

Restrictions Called "UnAmerican"

Kenneth Allen, senior vice president of the Information Industries Association, considers the restrictions "unAmerican." He said, "I doubt that they have the legal authority, I don't think they should, and it's ineffective." Such a policy may actually endanger U.S. security by limiting the free flow of ideas and the ability of U.S. business to capitalize on them. "I think it really is inconsistent with the idea of free flow of information in our society," he said of the NASA list.

"If it is unclassified, I don't understand why it shouldn't be shared with anyone who wants it," according to Allen. He also doubts the effectiveness of the NASA policy, commenting, "If there is someone out there who wants it, they are going to get." Nor does he think American engineers need a headstart, stating, "I don't think they need a headstart. I've got confidence in their abilities."

Reprinted from the BNA Daily Report for Executives by permission of the publisher.

Copyright © 1987 by THE BUREAU OF NATIONAL AFFAIRS, INC., Washington, D.C. 20037
0148-8155/87/$00.50

Heiland admits he is "not sure" that the "no-no list" is working, saying, "It is, at minimum, a best effort to identify foreign interests."

"Tech Briefs" have been published privately since 1985 by Associated Business Publishers Inc., of New York. The arrangement provides for publication at no cost to the government. "Tech Briefs" is available "free to engineers in U.S. industry and other domestic technology transfer agents," Heiland said.

Since publication was commercialized in 1985, the NASA mailing list of 71,000 has expanded to over 140,000, according to Heiland. Audited circulation was 110,000 last June, but it is growing rapidly, according to Bill Schnirring, publisher of ABP, who said the list is now proprietary. His company accompanies the uncopywrited "Tech Briefs" it gets from NASA with advertisements and with editorial products prepared by ABP staffers, such as "Mission Accomplished," a column on technology transfer success stories.

"We don't send 'Tech Briefs' out of this country," according to Schnirring, but he noted that various trade and engineering publications reprint "Tech Notes" material and do send it overseas.

"I don't have a 'no-no list,' " says Schnirring, explaining that his staff turns down requests that are obviously from foreign companies, and that Heiland staffers also screen the subscription requests.

Heiland feels that the mailing list is "99 percent clean." Discoveries of subscriptions going abroad have been made "incidently," he said. Nor does Heiland's staff work with other federal officials to keep "Tech Notes" out of foreign hands. "Tech Briefs" can be obtained in public libraries, through the National Technical Information Service, and through companies that lease the NTIS data base.

"I don't care," Heiland commented. He points out that the Technical Support Packages are harder to get, since they are available only on request from NASA.

Professor On List Gets Name Removed

One of those included on the "no-no list" is Michael Radner, a Northwestern University professor, whose name was accompanied with the notation "involved in hi-tech transfer with Japanese firms." Radnor was surprised to learn from BNA of his inclusion on the list. "We try and find technology in Japan for Illinois companies. Our whole project is to help U.S. companies," he exclaimed, "so some idiot has managed to stand it on its head." His project is funded by the State of Illinois.

After being told about the list, Radnor called Heiland's office, found "the whole thing was a mistake," and said later that as a result of his call, he has been removed from the list.

A Toyota representative in Washington, D.C., commented, "We subscribed for two or three years and suddenly we sent a renewal in and they said we can no longer supply it to foreign companies." This was about a year ago, he recalled, and although the official said, "we'd like to get it," he added, "If we need some special report we go to the library to get it." He noted that "the definition of a foreign company is very ambiguous."

Another company on the list is Info Doc, Dulles International Airport, Va., whose president, Michael Saboe, said, "I don't know who put us on this list; it's curious, it may just look like we should be on the list." Saboe's firm relies almost entirely on a contract with the Department of Commerce to distribute federal information domestically and worldwide, and has a proprietary interest in paying careful attention to the desires of government officials.

When asked on occasion to obtain "NASA Tech Briefs" for a foreign client, Saboe's company writes a letter to Heiland noting the name of the country to which the information would be sent. Sometimes Heiland's office will ask to know the name of the requestor, and Saboe's firm will check with the client for permission to tell the government. "We may give country of company, depending on client, and ask him to make the call," according to Saboe.

Copyright © 1987 by THE BUREAU OF NATIONAL AFFAIRS, INC., Washington, D.C. 20037
0148-8155/87/$00.50

Such coordination with the government is routine, Saboe said. "We contract with the Department of Commerce, [so] there are certain restrictions on what we can distribute and they are pretty clear." He added, "It doesn't bother me one way or another."

Not only with NASA, but also with other agencies, Saboe's firm routinely provides information on the destination of the requested material, and abides by the agencies' answers. Not uncommonly, even for allies, the government answer will be to have the foreign country apply for the information through diplomatic channels. "That doesn't mean they don't get it," noted Saboe, who said that sometimes his firm makes independent judgments not to send information.

NASA Policy Has Roots In Space Act

A NASA legal expert who preferred to remain nameless said, "We do not necessarily believe it appropriate in all situations to make (information) automatically available to foreign industry—the Space Act leaves us discretion." Sometimes, information will be supplied through diplomatic channels or to a potential licensor, he said.

Besides relying on the Space Act admonition for NASA to "provide for the widest practical and appropriate dissemination of information concerning its activities and the results thereof," the official referred to a statutory statement that NASA's mission "is to preserve the role of the U.S. as a leader in aeronautical and space science and technology and in the application thereof to the conduct of peaceful activities within and outside the atmosphere."

David Shonyo, director of the Office International Affairs at NTIS, told BNA, "In general, we will honor any prohibition an agency producing documents puts on," but he said NTIS has not been asked to protect "Tech Notes" from foreign distribution.

There are a few general Commerce Department prohibitions on shipping information overseas, but no separate Commerce review of the content of data placed in the computer system. Shoyno said, "We depend on the source agencies to keep out of our system anything that is so sensitive it should not get out."

Shonyo, who was not aware of the "no-no list," admits, "It's a pretty leaky system." Such lists are "largely symbolic," in his view.

NTIS does not sell anything to the Soviet Union, Poland, Czechoslavakia, Afghanistan, Nicaragua, and Libya. Most of the restrictions are developed in Commerce's International Trade Administration, in collaboration with the Office of Trade Administration. There are partial restrictions on other countries. No magnetic tape products may be sold to Albania, Bulgaria, the German Democratic Republic, Hungary, or Romania.

About 23 percent of NTIS sales come from outside the U.S., mostly from Canada.

The NTIS collection was started with material captured from Japan and Germany after World War II, and even today, about 25 percent of its one million documents comes from outside the U.S.

-- End of Section C --

Copyright © 1987 by THE BUREAU OF NATIONAL AFFAIRS, INC., Washington, D.C. 20037

Information Industry Association
555 New Jersey Avenue, N.W., Suite 800
Washington, D.C. 20001
202/639-8262
Cable: INFORMASSN WASHINGTON

DECEMBER 16, 1986
FOR IMMEDIATE RELEASE

INFORMATION INDUSTRY ASSOCIATION BALANCING FREEDOM OF SPEECH WITH NATIONAL SECURITY

Recent events suggest that certain persons within the United States government are attempting to restrict or monitor citizen access to unclassified information that is now generally available to the public.

> On October 29, 1986, the President's National Security Advisor issued a new, extremely broad security classification for government information: "sensitive but unclassified information." Implementation of this definition, which includes "human, financial, industrial, agricultural, technological, and law enforcement information," would deny citizens the right to acquire government information which has traditionally been available to the public.
>
> On November 11, 1986, a senior Department of Defense official stated that privately owned, unclassified electronic databases would be reviewed for "sensitive but unclassified information" and that access to these databases may be restricted or systems installed to monitor who uses them. Such actions could severely limit the information available to citizens, have a chilling effect upon those who wish to acquire information, and curtail the ability of U.S. information companies to do business.
>
> Over the last few months, representatives from the Department of Defense, Central Intelligence Agency and Federal Bureau of Investigation have been visiting private information companies to ask questions about who is using their information and for what purposes. It appears that the national security community is attempting to intimidate information companies into restricting access to their information or policing who uses it.

These government actions appear to be in response to concerns that foreign access to information, especially where available through new technologies such as on-line databases, is a potential threat to United States national security. Although the basis for these concerns has not been publicly documented, it is apparent that the information in question is unclassified government and private sector information that any citizen can easily and legally obtain by going to a public library. Should there be legitimate national security concerns about foreign access to information, the protection of such information must be addressed in accordance with the democratic process of checks and balances. Individual government officials cannot be permitted to restrict the right of citizens to create, acquire, use, and disseminate information in a manner that contravenes Constitutional and statutory law.

- MORE -

INFORMATION INDUSTRY ASSOCIATION
STATEMENT ON "BALANCING FREEDOM OF SPEECH WITH NATIONAL SECURITY"
December 16, 1986

Classification of information for national security purposes should not be based upon the media in which the information is available. Information which is unclassified and available to the general public, such as in print through a library, must not be restricted or classified when it enters an electronic database.

Once government information is released to the public, the government should not restrict the right of citizens to access such information or require information providers to monitor who uses the information.

If Department of Defense and other government agencies are concerned that public access to unclassified information is detrimental to the national security, they should make public the full bases of these concerns.

All information users must be assured that their privacy and confidentiality are fully protected in accordance with law and the highest possible ethical business practices. Authors, publishers and other information producers and providers must be assured that their creation of information, or their use and dissemination of unclassified government information, does not subject them to government censorship.

Government agencies should not attempt to dissuade information companies from legal business practices through intimidation or coercion.

The United States has spent 200 years in achieving a balance between national security interests and the right of citizens to create, acquire, use, and disseminate information. Changes in this balance should take place in an open forum in which all citizens have an opportunity to participate. Such a forum is the Congress of the United States.

Testimony
of
Cheryl W. Helsing
On Behalf of
The American Bankers Association
On
H.R. 145--The Computer Security Act of 1987
Before
Committee on Science, Space and Technology
U.S. House of Representatives
February 26, 1987

Mr. Chairman and members of the Subcommittee, I am Cheryl W. Helsing, Vice President and Deputy Director of Corporate Security for Bank of America, and Chairperson of the American Bankers Association's Data Security Management Committee, and I appear here on behalf of the American Bankers Association. The Association's member banks manage approximately 95% of the banking industry's total assets.

Over the past 18 months, there has been a growing concern over the Federal Government's direction in influencing private sector data security. That concern is shared not only by the financial community, but by other industries as well. In numerous conferences and meetings conducted for data security groups, this topic emerges again and again as a major concern. At issue is the impact upon private sector security programs resulting from National Security Decision Directive 145.

Under NSDD 145, the Defense Department and the National Security Agency guide the development of security solutions for protecting private sector and civil sector unclassified information, as well as national security-related information. Continuation of this policy, we believe, will not be beneficial to either the government or private sector users.

The American Bankers Association supports H.R. 145 as a measure that will restore a balanced relationship between the Federal Government and private industry.

The first issue of concern is the move to protect all sensitive information in the same manner--business information, information of importance to the national interest, and classified defense information. Within both the public and private sectors, there is a need for a broad spectrum of information systems security standards, techniques, and tools. There must be a range of security "solutions" that can be matched to the value of the information being protected, and the nature of the threats. Outside of the classified and national security arenas, both the private and public sectors must select cost-effective security measures.

To use a simple analogy, to travel from Point A to Point B one could choose a motorcycle, a truck, or a tank. These vehicles vary widely in cost, and each is best suited to a different environment. Under NSDD 145 and the programs that have resulted from that directive, the range of computer security solutions being developed have been narrowly focused on the "tank" end of the spectrum. The danger in doing this is, the road to be traveled might not accommodate a tank, or the traveler might not be able to afford the price tag. Thus, the trip might not be taken at all.

A striking example of this danger can be seen in how the NSA's new Commercial Comsec Endorsement Program (CCEP) has had an impact on the financial industry. Banks have spent several years developing a new technique for assuring the integrity and authenticity of electronic funds transfers and other information called "message authentication." At the same time, the industry began to make significant use of encryption to protect the privacy of information being stored in computers and transmitted over telecommunications facilities. Both these techniques employ the Data Encryption Standard, more commonly known as DES, established by the National Bureau of Standards as a Federal Information Processing Standard in 1977.

The National Security Agency announced a new set of encryption algorithms under CCEP, and stated its intention of discontinuing existing DES equipment endorsement programs in January, 1988. The attendant publicity has caused widespread belief that DES is no longer a prudent safeguard, casting a shadow in its continued use. Yet after more than 10 years in the public domain, no one has yet succeeded in compromising the security afforded by DES. There is no evidence that indicates DES is near the point where it will be broken; if there were, there are simple changes that can be made to the way that DES is used that would dramatically increase the difficulty of the task.

Under the announced requirements surrounding the use of the new CCEP algorithms, they cannot be used by the financial industry as a replacement for DES. They cannot be used internationally or placed in equipment for use by non-U.S. entities. The algorithms will be secret, rather than public, which will make them unacceptable in some foreign countries, even if the NSA would allow their use overseas. NSA is considering the retention of control over encryption keys, which would result in an unacceptable transfer of responsibility for the security of our data to a government entity. Those conditions may be appropriate for national defense-related security, but are clearly inappropriate for use in the financial industry.

This put banks in a difficult position. Years of work and many millions of dollars devoted to encryption and message authentication efforts were jeopardized. The ABA Data Security Management Committee initiated dialogue with the National Security Agency in October, 1985 on this issue. We finally reached agreement last week that the NSA would continue to support the financial industry's use of DES-based technology until an acceptable replacement is available.

While pleased that the NSA was ultimately receptive to our needs and operational constraints, 16 months elapsed while we worked to educate the NSA about our business. Our industry has lost momentum in adopting improved security technology, and it remains to be seen if we can overcome the damage that has been done to the perceived security of DES-based techniques.

The way in which this issue arose brings us to another private sector concern with the mechanisms established by NSDD 145. The CCEP program was developed in secrecy, without any determination of the private sector's needs or constraints in using cryptographic safeguards. Information systems security solutions are being developed with the stated intent of having broad applicability to the private sector, yet there is no formal means to gather direct input about our needs or the characteristics of the business environments in which we must operate. The National Telecommunications and Information Systems Security Committee (NTISSC), which develops operating policies necessary for implementation of NSDD 145, does not have a single private sector representative despite the intent of applying the results of the directive to the private sector.

One of the most important aspects of H.R. 145 from our perspective is establishment of a formal mechanism for private sector communication and cooperation with Federal Government. The financial industry strongly supports creation of the proposed Computer Security and Privacy Advisory Board with its industry representatives. One recommended change, however, would be in Sec 19a, to add a new paragraph to read as follows: "Four members outside of the Federal Government who are users of the technology, and who have computer systems, management experience, including computer systems, security and privacy experience."

Another reason for our strong support of H.R. 145 is the continuation of security validation programs upon which the private sector relies. Computer and communications security technology is often complex. Verifying adherence to standards or validating the correct operation of security systems requires specialized knowledge and technical resources not available to most business organizations. Furthermore, the independence and credibility of government validation is extremely valuable to our industry.

Because of the critical nature of information security measures in our business, the financial industry assigns great importance to U.S. government certification or validation of the measures we select. It assures our management, boards of directors, shareholders, and customers that we are utilizing prudent and effective controls in our business. Without a government-certified data encryption standard and accompanying program to validate correct implementations of that algorithm, we would certainly not have progressed in adopting this technique and accepting cryptography as the standard control measure it is today.

The ABA also supports H.R. 145 because it places responsibility for non-defense-related information systems security activities with the National Bureau of Standards, an agency with a long record of accomplishments of proven usefulness to the civil and private sectors. Federal Information Processing Standards and special publications issued by NBS on computer security topics have been widely used and accepted as industry standards in both the public and private sectors. NBS staff have interacted openly with the civil and private sectors since the early 1970's and have exhibited an excellent understanding of the need to balance

security objectives with cost-effectiveness.
The rapport NBS has achieved with the financial industry is, in part, due to the major contributions they have made in the development of our electronic funds transfer security standsrds. Their work on these efforts has exemplified their grasp of our need for effective yet flexible security techniques.

At the same time, we recognize the tremendous expertise and resources resident within the National Security Agency. The NSA and NBS have worked cooperatively in the past, and should continue to do so in the future. We would recommend that this legislation include a clear statement of the relationship between the two agencies, to preclude future confusion about their respective roles.

The financial industry's view of that relationship is that the National Bureau of Standards should have primary responsibility for information systems security initiatives affecting unclassified information, while the Department of Defense would have primary responsibility for information systems security initiatives affecting classified or national security information. The National Security Agency should continue to serve as a technical resource to NBS, while NBS acts as primary Federal government liaison to the private sector. This assignment of responsibility would ensure that NSA's primary mission of national defense would not be diluted, yet continue to allow the technological resources of NSA to be utilized in support of civil and private sector needs. NBS would continue to take the lead in the arena where its effectiveness has been clearly demonstrated. The private sector could benefit from the expertise of both groups by channeling our requirements through the agency with which we have an established working relationship and a track record of successful results. This would restore the mutually beneficial and synergistic relationship that existed between the private sector and Federal government prior to the changes wrought by NSDD 145.

In conclusion, the American Bankers Association endorses H.R. 145 as a means of reversing the counterproductive impact of NSDD 145 and its resulting policy programs upon the financial industry. We further believe the information systems security programs established by the legislation are vitally needed within civil government, just as they are within our business environment, and that the National Bureau of Standards is the best-qualified agency to provide leadership.

I thank you for the opportunity to present our position, and would be happy to respond to your questions.

Statement

of

Geoffrey W. Turner

Communications Security Manager

BankAmerica Corporation

to

The Subcommittee on Science, Research and Technology

House Committee on Science and Technology

Hearings on

The Computer Security Act of 1987

H.R. 145

February 25, 1987

As manager of communications security for BankAmerica Corporation, I am responsible for policies to secure data communications in the corporation's data systems and networks. I also represent BankAmerica on several national committees which establish data security standards both for the financial services industry and for other industries. Prior to joining BankAmerica, I served fourteen years as an Intelligence Officer in the United States Navy, where I gained extensive experience in the security of information systems and communications. It was my involvement with information security in these two environments that drew my attention to the interrelationship of federal and private sector information security policy. It is that interrelationship which brings BankAmerica here today to testify in support of H.R. 145.

Since the early 1980's, BankAmerica has been a strong supporter of a financial services industry effort to develop information systems security standards through the American National Standards Institute. This ongoing program has resulted in the development of standards which allow institutions to secure such sensitive information as electronic funds transfers. These standards were developed from a perspective significantly different from that upon which the protection of national security information is based. In BankAmerica, for example, information is viewed as a corporate asset, with a defineable dollar value and which is thus protected just as we protect other valuable corporation assets. But because we are a business, we cannot spend more money to protect an information asset than is cost-justifiable. The security standards our industry has developed, and the technologies which support them, are inherently compatible with this pragmatic approach to information systems security, and work very well in our business environment.

The Department of Defense, which has responsibility for the security of classified national security information, has developed security techniques and technology quite different from those of our industry. Since the definition of information classified TOP SECRET is "information, the unauthorized disclosure of which would cause extremely grave damage to the security of the United States," it cannot be assigned a monetary value. It follows that TOP SECRET information must be protected without regard to the cost, and this is reflected in the resulting design of techniques and technologies. This basically absolutist approach to information systems security, while very appropriate for the national security environment, does not work well in the necessarily more pragmatic private sector.

This dichotomy of information systems security philosophies and environments is a major reason why the private sector has viewed National Security Decision Directive 145 and its related programs with increasing concern. NSDD 145 emplaced the Defense Department as the national program manager of National Telecommunications and Information Systems Security Committee programs to address the security of unclassified but sensitive information. This mandate covers the civil sector of government, and to an as yet undetermined degree, the private sector as well. Yet, as I have described above, the Defense Department's expertise is not universally applicable to these other environments. Many of the security techniques advocated by the National Security Agency for the non-defense environment are unworkable for reasons of either excessively high cost, unacceptable restrictions on their use, unacceptable degrees of NSA involvement in their operation, or general operational incompatability with many non-defense environments. As a result, some of its well-intentioned actions under the NSDD 145 mandate have worked instead to slow down and complicate the securing of information systems in the civil and private sectors.

A primary example of this is the security of electronic funds transfers (EFT). EFT security standards developed by the financial services industry, are based upon a cryptographic algorithm called the Data Encryption Algorithm, more well known as DES, established by the National Bureau of Standards in 1976. These industry standards are being implemented in the private sector to protect electronic funds transfer systems, and have also been adopted for that purpose in civil government programs such as those in the Treasury Department and the Federal Reserve System.

In 1985, the National Security Agency stated that by 1988, it would no longer provide certification support to DES technology. Instead, it was instituting a progam of new algorithms, called the Commercial COMSEC Endorsement Program, which it viewed as a successor to DES. After a review of the CCEP, BankAmerica determined this would not be a viable replacement for DES in the financial services industry, for a number of reasons, all related to the fundamental differences in security philosophies. The NSA's apparent vote of no confidence in DES had the effect of discouraging development of DES technology and investment in it by financial institutions. The net result was a slowdown in the securing of this nation's electronic funds transfer systems, certainly not the intention of the NSA or the Department of Defense. This contrary relationship between intent and effect is an example of the serious consequences of misplaced responsibility for information systems security policy within the federal government.

The financial services industry security standards were developed with the indispensible technical participation of computer security experts from the National Bureau of Standards. They provided and continue to provide the independent, unbiased and state-of-the-art technical knowledge without which these security standards cannot be developed or implemented. The Bureau of Standards is playing a vital role in the Treasury Department's program to implement these standards in federal EFT systems. It is due to the NBS' length and breadth of non-defense sector experience in information systems security, that they are able to provide this critical support to both the private and civil sectors.

With the advent of NSDD 145 organizations and programs, the relative roles of the Department of Defense and the National Bureau of Standards in information systems security policy for the federal government and liaison with the private sector have become unclear. BankAmerica believes that the National Bureau of Standards represents the best source of non-defense information systems security expertise in the federal government, and should play the leading role in the development of civil government policy. The non-defense perspective of the NBS provides that agency with the ability to develop information systems security standards well-suited to civil government agencies' real needs in a cost effective manner. The valuable technical expertise of the National Security Agency would still be available to civil agencies, but through the coordination of the NBS, more experienced in the non-defense environment. In addition, the NBS, as an open agency with many ongoing joint civil-private sector programs in computer security, is better able to effectively interact with its constituency than is a basically closed agency such as the National Security Agency. This much more open relationship between the standards setting agency, NBS, and those responsible for implementing the standards will go a long way towards preventing costly missteps, such as the DES controversy. The success of the NBS in generating information systems security standards for the federal government and in supporting private sector standards development makes it eminently qualified to meet the requirement of this bill.

In addition, the creation of the Computer System Security and Privacy Advisory Board is an important step to establishing the necessary liaison of security efforts between the federal government and the private sector. It is the absence of these functions in the NSDD 145 and NTISSC environments that has led to the problems described previously. BankAmerica strongly supports this provision of the bill, for it will enhance the security efforts in both private and civil sectors and will also generate synergies of lower costs through use of common techniques and technologies. This closer cooperation will also better meet the intent of NSDD 145 to advise, assist and encourage information systems security in the private sector to protect national interest information in the private sector

In conclusion, BankAmerica Corporation strongly supports the passage of H.R. 145 and endorses the expansion of the role of the National Bureau of Standards in federal information systems security policy. We believe enactment of this bill will generate a higher degree of information systems security in the civil government at lower cost to the taxpayers. It will also greatly assist the private sector in implementing secure information systems and protecting information that is in the national interest, again at less cost to the American public.

BankAmerica and I thank you for this opportunity to present our views on this vitally important subject.

Mr. WALGREN. Let's call, then, the last group as a panel: Jerry Berman, Chief Legislative Counsel, the American Civil Liberties Union; John Richardson, Chairman of the Committee on Communications and Information Policy for the Institute of Electrical and Electronics Engineers; and David Pronko, President of PE Systems.

If all of you could come forward again, as Mr. McCurdy said, we know that you have different perspectives, but we want to hear you as a panel, and your written statements will be made part of the record. Please feel free to summarize as concisely as possible to focus on the points that really cry out to be communicated and also know that those mikes need to be pulled in and spoken into very directionally, or they really just don't plain pick up and let the folks in the back of the room hear.

Let's start then with Mr. Berman.

STATEMENTS OF JERRY BERMAN, CHIEF LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON, DC; JOHN RICHARDSON, CHAIRMAN, COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY, THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC., WASHINGTON, DC; AND DAVID PRONKO, PRESIDENT, PE SYSTEMS, INC., ALEXANDRIA, VA

Mr. BERMAN. Thank you, Mr. Chairman.

I know that you've been listening to a lot of witnesses. I have a very long statement, which I am submitting for the record. I think it's all very important, but I won't read it to you today.

Let me try and just summarize and make some points. There is an awful lot of confusion, a lot of it caused, I believe, by the Administration's presentation of what they think NSDD-145 says and what they purport to be doing and what, in fact, they are doing. I think they are quite different.

When NSDD-145 was promulgated, we testified before this committee that it represented a major, significant change in government policy, because it, in effect, put the military, DOD and the CIA and NSA, in charge of information policy and information security for the whole government, not simply for classified information, but for unclassified information which they termed sensitive, which the directive leaves very vague, and also with an advisory or outreach role to the private sector.

We have no quarrel with the issue that there is a problem of unauthorized access to computer and information systems or to communications systems, but the wisdom of allowing the military to have the lead role with respect to civilian agencies and the private sector, we believe, raises troubling questions about the free flow of information and open government.

The job of the military, if they do it properly, is to keep secrets, and their penchant for secrecy, when applied on the civilian sector and the private sector of government, could lead to more restrictions on information.

When we testified and said that those were our fears, we were pooh-poohed by Mr. Latham, and they continue to testify that that's not what NSDD-145 is about; it's to protect against the penetration of information systems and communications systems, "That's what we're doing," and number two, that it has no—that "we have no real role in trying to limit unclassified information, and that our definitions are very narrow."

Let me just take you through three—Since that directive, they have expanded the definition of "sensitive information," as the gentleman from the Bureau of Standards testified, to encompass almost all government information. It's not simply classified information or national security-related information. Sensitive information is unclassified information which may affect any federal interest.

Number two, they are reaching out to the private sector, not just government contractors who are doing defense work, but, as the gentleman from Mead Data says, they've come to NEXUS, which compiles newspapers, and said, "What's in your system? Can you monitor who has access here? Can you limit access to unclassified information in your system, because the Soviets might get it." It's a very effective means of getting information if it's in computers.

Well, under the Freedom of Information Act and under the First Amendment and in an open society, the Soviets are going to get a hold of a lot of unclassified information. But because they do is no justification for controlling it or limiting access to it.

Yet right now, the defense agencies, under NSDD-145, every agency gets to make its own decision about what information is sensitive. But under the coordination of NSA, the tendency of bureaucracies from HHS to Agriculture, I believe, will be to restrict a lot of information in order to err on the side of protection. So they will put on more restrictions on the civilian side of government.

The private sector has already said, "We want to avoid the hassle; we've taken NTIS off our system." In the private sector, a visit by NSA or an intelligence agency, which I believe is a form of foreign intelligence surveillance in the United States, which is barred by Executive Order 12333 on the role of NSA in the United States, has a chilling effect on a company, because it says, "We think adversaries are getting access to this information, and will you cooperate with us?"

Well, the implication is that "if you don't cooperate with us, you're not being patriotic; you're violating the national security, and you're on a bad list down at NSA." And I believe that whether they call it a "bad list" or not, they are keeping an account of security—who's taking the appropriate security measures.

Now the third point is that they've said, outside of this voluntary outreach, they have spoken in public and to the Information Industry Association and said quite plainly that if voluntary measures don't work, they are prepared to take information, unclassified information again—and I'm always speaking about unclassified information—out of NTIS and other government data base system, to use licensing restrictions to try and limit the dissemination to certain companies.

They, for example—they already have a list of American companies that they don't want to give information to, because they have foreign clients. Under the Freedom of Information Act, there is no distinction between foreigners and Americans, and information that's public is public. But they are making distinctions with respect to electronic data under a very interesting scheme which says that the Government has some sort of de facto copyright licensing control over electronic data, if they're prepared to make a hard copy available.

It's a very complicated argument, and it's in my testimony. But they are prepared to talk about gateways, putting monitors on government computer systems to see how systems are being used by citizens, how it's being accessed, what's being searched, gateways to try and limit which citizens and which organizations gain access to unclassified information in government systems, and to encourage the private sector to follow suit, and if they don't follow suit, to do as they have done and with conferences, academic communities and research facilities: They try to use the threat of prosecution under the export control laws, and threaten that kind of prosecution and get them to stop or to limit access to unclassified information.

We believe that H.R. 145 should be passed. We would rescind the directive. H.R. 145 does that in the sense of returning civilian control to the civilian side of government.

And then Congress has to wrestle with a second question, which the Congressman mentioned, which is, what definition of sensitive information do we want around here?

And I think that there is already a definition in law, and the definition is "classified information or information which is otherwise protected from disclosure under current statutes of law." If it's classified, protect it. If it's proprietary, trade secrets, there are statutes on the books. If Congress wants to create a new class—a new set of information which they don't want the public to have, pass a statute. But don't have a broad, overbroad, and subject to vagueness definition of sensitive information floating around in a statute, whether Commerce has jurisdiction or whether Defense has jurisdiction. I think it's going to lead to restrictions on information, less free access to information, less public right to know, less open government, and that's why we think the work of this committee is very important.

Thank you.

Mr. WALGREN. Thank you, Mr. Berman. We appreciate that testimony.

Mr. Richardson.

Mr. RICHARDSON. Thank you, Mr. Chairman.

I'm going to make some points which have already been made, because I think they deserve stressing. I hope you will bear with me, and I will be as brief as I can.

NSDD-145 limits itself to information that would adversely affect the national security interest if it were lost, and it admits both government and non-government information into this class. We think that that's wrong. The Government should not concern itself with non-government information.

The Poindexter Memorandum came along and broadened that definition of sensitive information to other Federal Government interests as well as national security interests, as Ray Kammer and Jerry Berman pointed out. We think that that broadening is going to make problems.

Both NSDD-145 and the Poindexter Memorandum want to provide guidance to all federal agencies from the Director of the National Security Agency. We think that that's wrong.

H.R. 145 would separate the protection of computer systems from dealing with national security information from that of computer systems dealing with non-national security information, and it would give a civilian agency responsibility to assist the other civilian agencies. We think that that's right. So now let me stress the main points of our position.

We oppose government categorization and protection of non-government information.

Second, we endorse the intent of H.R. 145 that a civilian agency, rather than a defense agency, should assist other civilian agencies and the private sector in the protection of computer systems, and the reason is to avoid applying national security biases in other areas.

Third, we believe that the Poindexter Memorandum should be rescinded as too broad and that Congress should require that practical, uniform guidelines be publicly developed and limit the amount of government information designated as sensitive and the inevitable abridgment of access to such information.

And the fourth point of our position, we think that studies ought to continue to better ascertain the balance between the costs and the benefits of this protection. The costs and benefits have appeared fuzzy in this hearing.

Let me explain why IEEE cares about this. Lots of its members have expertise in this area, so we can help. But more importantly, lots of our members want access to government information as a part of their profession, and they are concerned with limitation of access. Also, government actions may have influence on the protection policies and practices that may ultimately be required of or adopted by the private sector, and most of our members work in the private sector. So we care.

I have identified five questions that are worth focusing on. I would just like to mention them and make a brief comment.

First, is there such a thing as sensitive, but unclassified information in the sense of the Poindexter Memorandum?

We concede that there is, but in previous testimony before this committee in 1985, I urged extreme restraint in the identification of such information. The definition used in the Poindexter Memorandum is not extreme restraint. Indeed, the Poindexter Memorandum gives the classifiers—namely, the agency heads—essentially unconstrained powers in identifying that information and unconstrained powers in laying on protection. Agency heads should be required to follow guidelines that are developed from careful rulemaking. I think that's the way to narrow this definition to a workable dimension.

The second issue is, how do we go about protecting the information?

Well, obviously, you protect the systems that handle it. In protecting the systems that handle it, it's been adequately pointed out by other speakers that you limit access to those systems. You limit access by erecting barriers to their use, not only for those we wish to impede, but for those that we do not in some degree. That's such an important point that I want to stress it again.

The third issue is, what about the costs of protecting too much information and the costs of abridging access?

Well, it's obvious that the more you seek to protect, the less access you allow. That's the reason why the class of this information should be as narrow as possible. The IEEE thinks, in this regard, that the unabridged dissemination of unclassified scientific and technical information is crucial for the continued advancement of U.S. industry, and we oppose restraints on its exchange.

The fourth question worth mentioning is, are there adequate guidelines for a workable definition? And we say that the guidelines are inadequate. I don't have a suitable definition here, in response to the question I'm going to get from the gentleman from Missouri, but we have to work on that. I have to say that the definition in H.R. 145—I agree with Ray Kammer—the definition in H.R. 145 is just as broad as that in the Poindexter Memorandum, and it's not quite satisfactory.

The fifth and final question is, should there be separation of responsibilities between national security affairs and other Federal Government interests? I've already said that we favor a clean division of those responsibilities.

Mr. Chairman and members, that summarizes the main points that I think need to be made, and I'll be happy to take any questions.

Mr. WALGREN. Thank you very much. Let me recognize the gentleman from Missouri, if he would like to raise anything at this point. I understand you have a commitment that you have to meet, and we certainly appreciate the interest you've taken in this whole issue.

Mr. BUECHNER. Thank you, Mr. Chairman.

You anticipated my question. I would have asked the same thing about a definition of "sensitive" of both of you, and I recognize the problems it creates.

I have left with the chairman a couple of questions for Mr. Pronko.

Thank you all for attending.

I have to be interviewed about the Tower Report. It seems to be of some sort of interest back home. [Laughter.]

Mr. MCCURDY. Let's turn to Mr. Pronko, if you wish to summarize your testimony, we'd be happy to hear it at this time.

Mr. PRONKO. Mr. Chairman, I'm not going to read any prepared testimony. I just wanted to make a few comments on some ideas I've heard here this afternoon.

Basically, PE Systems—I'm President of PE Systems and we bridged the gap between the private sector and the military sector. We make encryption devices using both the DES standard and the new algorithms developed by NSA, under the CCEP program.

I'm rather appalled by the American Banking Association and their lack of knowledge of what the CCEP is. It is not an algorithm, but what it is is a program to get a series of algorithms out in the field, inexpensive devices to be used as you want to use them. I'm not here to defend NSA or the CCEP program, but what

I am here for is trying to give the Committee some of my knowledge on attempting to market to both sides of the field.

What we have found is that it is not so much a total security matter. The DES algorithm is a very good algorithm. We manufacture several products with it, as I have said. We have, as I said, a CCEP item which is good in the classified world up to the Secret level, but what we have found when we have gone out into the market is a lack of education in both the military, would you believe it, along with the private and the other Federal Government agencies.

They really do not know how to handle the new programs, any part of it. What we have found also is that within the private sector and the other non-DOD portion of the Government, the big brother feeling, as we have heard several times today.

One thing I might suggest for that, it's not so much the algorithm you use, I say they are all good, they are all excellent algorithms, it's who is supplying the keying material for the algorithms themselves. If we can get NBS and NSA to come up with a good method of supplying the keying algorithms, where the users would feel that they have control of what they are doing, then I think we have something to work with.

Mr. WALGREN. Mr. Pronko, the two questions that the minority wanted to raise and in view of the fact that you have worked both with the NSA and NBS for several years, would you characterize the strengths and weaknesses of those agencies with respect to providing security for military computers on the one hand and civilian computers on the other?

Mr. PRONKO. I'll try but remember, I'm coming at it from a rather narrow viewpoint, from the communications security point of view alone, not the total computer security world.

From the communications security point of view, I feel that NSA has a—my own personal view—a much more pragmatic approach and a more methodical approach on handling the communications security. At NBS, you have really more of a laissez faire approach to it, and here again, it is probably brought about by private industry working within that system.

Mr. WALGREN. Let me ask you a second question that was provided by the minority, and they asked, under the provisions of H.R. 145 with respect to computer security training, which agency, the National Security Agency or NBS, do you feel could best provide computer security training?

Mr. PRONKO. At this stage from what I've seen and in my earlier comments, I'm not sure either has a leg up on the other as far as the computer security training right now. It seems that the NSA within the last few years has gained a foot hold in that arena, due to their programs.

Mr. WALGREN. But I gather from that there would be nothing inherently different in each agency that would say one——

Mr. PRONKO. I wouldn't think so.

Mr. WALGREN [continuing]. Would not do as well as the other?

Mr. PRONKO. No. I wouldn't think so except maybe one has a little edge right now. They have more people available and have been doing it a little longer.

Mr. WALGREN. The gentleman from Oklahoma.

Mr. McCurdy [presiding]. Thank you, Mr. Chairman. Gentlemen, thank you for your appearance today. We certainly appreciate your input and having your statements in the record.

Mr. Berman, you made one statement as I came back into the room that caught my interest and that was you asserted that visits by NSA personnel to private companies was a violation of the National Security Act, restrictions on the intelligence community from having surveillance when operating within the continental United States.

Is that a position that you have researched and have a paper on?

Mr. Berman. Let me give you my—I don't have a paper on it but I've done a lot of work in the intelligence area. I've been around on the national security surveillance issue and worked on both the Carter Executive Order on intelligence activities and on the Reagan Executive Order re-write with the intelligence committees.

It is clear under Executive Order 12333 that the role of the National Security Agency is overseas. It is a foreign intelligence agency. It has a communications security function focused abroad. It has no domestic security or intelligence functions with respect to investigating American citizens. That is left to the FBI.

Now, while there may be an argument—I think this is an intelligence program to the extent that NSA is visiting firms on national security grounds to determine whether or not they are taking adequate measures to protect data which they consider sensitive, suggesting one way or another that they make changes in their system, and I think of necessity, starting to maintain some record down at the agency, of which firms they visited, what information is sensitive, I mean this includes banks, insurance companies and the like, which raises a file issue.

Mr. McCurdy. Would you have the same problems with the FBI? Would there be the same problem for the FBI?

Mr. Berman. The FBI has a counterintelligence jurisdiction in the United States and also has a positive foreign intelligence, which is defined, what other foreign countries are doing, what kind of access they do, without any targeting of citizens.

Now, it's possible to make an argument that this directive is amended by NSDD-145, which comes after the Executive Order on intelligence, and therefore, amends the authority of NSA and gives it this domestic role, but you can argue both ways but I think there was wisdom in keeping NSA overseas and the argument behind it is NSA has no charter, doesn't operate under the same accountability rules as other agencies of Government, like the FBI, not with the same checks and balances. It's very secret.

I don't think its name was public until 1962. It never testified before the Congress until 1975 and then about some abuses, and while I don't think NSA is engaged in any intelligence abuses, such as wire tapping or eavesdropping, if they do anything wrong, it is impossible to sue them. It is impossible to sue them because of the secrecy privilege which extends to the sources and methods which they employ. They are beyond the civil law of the United States.

That's a long answer to your question.

Mr. McCurdy. Well, as I've stated before, it is worth looking at. I seriously think it is worth it. Before this Subcommittee, I chaired a Subcommittee on Oversight within the Intelligence Committee. I assure you that even though it is not done in the same situation or the same circumstances, there is oversight of the National Security Agency.

Mr. Berman. I will say that staff on both the House and Senate Intelligence Committees have begun to——

Mr. McCurdy. That's the first I had heard of it, to be frank. I wanted to hear your views on it. I think there may be some grayness in there.

Mr. Berman. Well, I mean, there's another gradation to it, which is, you know, NSA—they keep wondering why there is so much puzzlement about their role, and I'm not saying it is because of past abuses, but they have a conflict of interest in some sense. Their first real effort in the communications security area was to block private efforts to develop cryptography methods, which would provide greater security. Here they are saying they are now a public agency providing secure phones, new encryption devices, and you know, we are a phone call away, and we are just your ready, new public agency, and we are in the business of giving you security.

Mr. McCurdy. There's no secret there are a lot of bastard agencies within the Federal Government that don't have a clear line of lineage and we are not exactly sure who they are responsible for. I think on the computer security directive, I mean, they created one. We are trying to sort that out. I don't think anyone, certainly within this body, is trying to stop the flow of public unclassified information, but at the same time, we are charged with maintaining the national security and we want to protect the sensitive and classified areas.

I don't argue with your point.

Mr. Berman. For NSA and the DOD under NSDD-145 to be worrying about limiting access or dissemination of unclassified information, it seems to me far afield from the original scope of that directive, and if you look at the history of how that directive arose, there were efforts to put authorization language into the defense authorization bill in 1984 which said there was a national crisis which required a coordinated approach that NSA should have that control, and there was a big fight and it was taken out of that bill.

There is a bureaucratic effort here and I think NSA and DOD want to battle and this legislation is an attempt——

Mr. McCurdy. Well, they want a temporary battle. As I said earlier, sometimes a promptitude decision in the legislature is more often an evil than a benefit. I think through the exercise that we may come out a little stronger. I don't think anyone is doing the bidding of NSA or the Department of Defense.

I think we have made substantial progress in the last few weeks. I think probably it is partially attributable to the fact that some of us who have jurisdiction in other areas over these people have said, you better get your act together. I sense that message has been received.

Mr. Berman. We are having a consultation jointly sponsored by the scientific associations, the information industry, bankers, a very broad interest in this issue.

Mr. McCurdy. We want to avoid duplication. We want to protect your tax dollars as well as your freedom. I don't sense there is a major problem there.

Gentlemen, I have no further questions. I'm left. It's me. Again, we appreciate you taking the time to come today and provide your information and your testimony. It has been very helpful. We will leave, without objection, we will leave the record open for ten days in order to have questions submitted in writing to the witnesses. We will do our best not to burden you with lengthy questions from the staff, but there may be some areas that we would like to follow up on. If you could, we would appreciate it. Thank you again.

We stand adjourned.

[Whereupon, at 4:54 p.m., the Subcommittee recessed, to reconvene at the call of the Chair.]

[The prepared statements of Mr. Berman and Mr. Richardson follow:]

PREPARED TESTIMONY

AND

STATEMENT FOR THE RECORD

OF

JERRY J. BERMAN
CHIEF LEGISLATIVE COUNSEL
AMERICAN CIVIL LIBERTIES UNION

ON

NATIONAL SECURITY DECISION DIRECTIVE 145
TELECOMMUNICATIONS AND AUTOMATED SYSTEMS SECURITY
AND

H.R. 145
THE COMPUTER SECURITY ACT OF 1987

BEFORE THE

HOUSE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

FEBRUARY 26, 1987

Mr. Chairman and Members of the Committee:

We want to thank you for requesting us to testify today on H.R. 145 and National Security Decision Directive 145. As you know, the American Civil Liberties Union is a non-partisan organization of over 250,000 members dedicated to the defense and enhancement of civil liberties guaranteed by the Bill of Rights.

I. Introduction:

First of all, Mr. Chairman, we want to commend Mr. Glickman and other Committee sponsors of this legislation for introducing H.R. 145, "the Computer Security Act of 1987" which attempts to rectify some of the serious civil liberties dangers posed by President Reagan's secret National Security Decision Directive 145 on Telecommunications and Computer Security (NSDD 145) promulgated in September 1984.

II. Brief Overview of NSDD 145:

NSDD 145 supersedes President Carter's 1979 Directive on telecommunications security (PD 24) and signals a major change in government information policy. The Carter Directive authorized the Department of Defense to protect classified telecommunications systems and the Department of Commerce to protect unclassified telecommunications systems. Now NSDD 145 places authority for all government communications and computer security systems which communicate or store classified and so-called "unclassified sensitive information" under the jurisdiction of the Department of Defense (the Executive Agent), and the super-secret National Security Agency (National Manager).

It authorizes these defense agencies to coordinate protection for civilian agency communications and computer systems which communicate or store "unclassified sensitive" information and also authorizes DOD and NSA to advise the private sector on information system security.

III. The Potential Danger of NSDD 145:

We testified on NSDD 145 in the last Congress and expressed serious reservations about the Directive's potential adverse impact on the free flow of information and open government. While we conceded the underlying rationale for NSDD 145--the need to improve communications and computer security against unauthorized access and hostile penetration--we shared your view that it was unwise and unwarranted--under the Brooks Act (89 306)--to authorize military agencies to coordinate or implement policies or procedures to protect unclassified information systems operated by civilian agencies or private industry. As Rep. Brooks aptly stated at the time:

> "Since it is a natural tendency of DOD to classify everything, it would be impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information."

We testified that if DOD and NSA did their job well--and their information protection mission is keeping secrets--open government would be jeopardized. Without an appropriate balancing of interests between the need for secrecy and the need for open government, we feared military control would lead to more restrictions on public access to unclassified information; more compartmentalization of information; more security measures for civilian agency personnel (background checks, prepublication secrecy agreements); and more sophisticated high-tech authentication systems. These are measures government requires for the protection of classified information but which threaten the free flow of public information essential to the workings of democratic institutions if applied to cover unclassified information.

Our concern was not hypothetical. In the name of "national security," the Reagan Administration was already embarked on a wide ranging effort to control access to what it terms "unclassified sensitive information" at universities, at scientific conferences, and in the media. Using visa restrictions, threat of prosecution under the export control laws, broad interpretation of the espionage laws, threats to withhold government contracts or grants, and other measures, the Reagan Administration had:

-- undermined academic freedom by requiring universities to restrict access on their campuses to keep designated foreigners from visiting laboratories engaged in unclassified research and from enrolling in specific research programs;

-- restricted the free flow of information by preventing the presentation of scientific papers at conferences;

-- inhibited free speech by interpreting and applying the espionage laws to cover publication of information by the press; and

-- limited the public's right to know by seeking to expand the exemptions for information disclosure under the FOIA to permit the withholding of unclassified information related to national defense and using authority under the Executive Order on Classification (E.O.12356) to reclassify information made public but then retrieved from a library.

IV. A Clear and Present Danger:

We now know that our concerns about NSDD 145 were more than justified. Pursuant to NSDD 145, our military and foreign intelligence agencies are extending military control over access to public information in government and commercial databases. Unless halted, this militarization of the information process threatens the free flow of public information, scientific inquiry, competitiveness of the information industry, and open government. Below we discuss how NSDD 145 has been interpreted and discuss these policy consequences.

V. The Expanding Scope of NSDD 145:

As you know, when the Department of Defense testified before the House Government Operations Committee, officials were adamant that the Committee and public witnesses were misinterpreting the purpose and scope of NSDD 145. However, Administration declarations meant to assure the public of the narrow scope of NSDD 145 have been followed by contradictory statements broadening the scope of the Directive.

The general thrust of Administration policy clarifications has been to expand the role of the military in protecting or controlling civilian agency and private information systems by: (1) expanding the definition of unclassified sensitive information which requires protection in information systems; (2)

enlarging the military's "advisory" role in the private sector; and (3) most alarming, defining information protection measures to include not only those designed to prevent unauthorized penetration and access to information systems but measures designed *to control and limit the dissemination of "unclassified sensitive information."*

1. Sensitive Unclassified Information:

In his September 1985 testimony before Congress Donald Latham, Assistant Secretary of Defense Command, Control, Communications and Intelligence and Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC), established under NSDD 145 to develop and implement communications and computer security policies, stated:

> "Specifically, it (the NTISSC Subcommittee on Automated Information Systems Security) separates unclassified but sensitive information into two categories: sensitive national-security related; and sensitive non-national security related. The purview of NSDD 145 is *only* for the former category. Let me reiterate that NSDD 145 *does not cover unclassified but sensitive non-national security-related information and therefore, it in no way restricts, controls, or manages the activities of other federal agencies who have responsibilities in non-national security related areas*...." (emphasis original)

Within months, as documented in the House Government Operations Committee's August 1986 report, the National Security Agency, which acts as National Manager under NSDD 145, expanded the scope of NSDD 145 to include non-national security related information in both public and private information systems:

"NSA...announced that it was merging its

> Communications Security (COMSEC) and its Computer Security (COMPUSEC) organizations into an integrated organization called Information Security. In its announcement, the following was stated: 'The responsibilities of the new organization (within NSA) are being broadened under the auspices of National Security Decision Directive 145 to include all computer security and communications security for the Federal Government and private industry, including the protection of classified information; and non-national security sensitive information." (emphasis supplied by the Committee)

On October 29, 1986, Admiral John Poindexter, then head of the National Security Council, issued National Telecommunications and Information Systems Security Policy No. 2 (NTISSP 2). NTISSP 2's definition of unclassified sensitive information encompasses an extraordinary range of information in the public domain from national security related matters to information which may affect any "other federal interests."

> "Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens."

On January 7th of this year, Donald Latham wrote a letter to the President of the Information Industry Association designed to allay IIA's concerns about the scope of NTISSP 2. His description of sensitive information covered by the Directive directly contradicts his testimony before the House Government Operations Committee which unequivocally excluded from NSDD 145 jurisdiction privacy, law enforcement, and other such information or information systems. His letter states:

> "By way of example, the type of information in systems we want to protect from unauthorized access includes IRS records, which are neither classified nor national-security related. Another example of systems which may be appropriate for protection are those which process information pertaining to law enforcement operations."

2. Government and Commercial Data Bases Included

Pursuant to NTISSP 2 all government systems containing unclassified sensitive information as defined are covered by NSDD 145's mandate. NTISSP 2 applies "to all Federal Branch Departments and Agencies, and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information."

All private sector information systems which contain sensitive information as defined under NTISSP 2 may also come within the purview of NSDD 145. On its face, NTISSP 2 appears only to apply to government contractors. This limitation may be more apparent than real.

First, non-contractor private sector systems which contain unclassified sensitive information which may adversely affect national security are included within the scope of NSDD 145. The Directive itself makes no distinction between contractors and other private sector systems for this category of information. The Department of Defense in a September 1985 report, Soviet Acquisition of Military Significant Western Technology: An Update identifies both government and commercial databases as a principle means by which foreign adversaries acquire advanced western technology and suggested possible measures to protect and control systems which contain such "sensitive information":

> "Unclassified technical documents from all countries--including engineering analyses and research results--are targeted by Soviet intelligence and other collectors because of their value to Soviet engineers seeking creative designs and alternative engineering approaches."

After giving examples of Soviet acquisition from on-line databases of space shuttle technology from NASA-funded defense contractor studies from online databases, the Report expands the Pentagon's concern to include not only specific technical data acquisition but, non-specific, generalized aggregate acquisitions of unclassified data which may threaten national security:

> "The individual abstracts or references in government and commercial data bases are unclassified, but some information, taken in the aggregate, may reveal sensitive information concerning U.S. strategic capabilities and vulnerabilities....The public and private document clearinghouses... established to efficiently index and disseminate the results of government and government-sponsored military-related technical research...are a fertile ground for KGB, GRU, and other collectors. In recent years, the growing use of electronic data bases has provided the Soviets with an even more efficient means of identifying and procuring such unclassified technical information needed by Soviet designers. (emphasis supplied)

There are indications that private communication and information systems which contain "non-national security" related unclassified information may also come within the scope of NSDD 145. Donald Latham, in testifying before a Subcommittee of the

House Science and Technology Committee in June 1985 explained the "general climate" that led to the promulgation of NSDD 145:

> "Virtually every aspect of Government and private information is readily available to our adversaries--unfriendly governments and international terrorist organizations are finding easy pickings in the flood of unprotected telecommunications and automated data processing information afloat in this country."

Walter Deeley, then Director of Communications Security at the National Security Agency, testifying at the same hearing, called for a cooperative effort between government and private sector to protect "national" and "private secrets:"

> "The NSA's responsibilities as National Manager are wide-ranging and vital to the security of our nation's telecommunications and information systems. However, they are not to be viewed in isolation, for without the active participation and support of all elements of the Government, and that portion of the private sector which handles sensitive Government (and non-Government) information, our national and private secrets will remain exposed to any adversary."

In December 1985, as reported by the House Government Operations Committee, NSA merged its communications security (COMSEC) and computer security (COMPUSEC) organizations into one organization (Information Security) responsible for communications and computer security for the Federal government and "private industry, including the protection of...non-national security sensitive information."

In the past year, both the National Security Agency and the Central Intelligence Agency have visited commercial database firms which operate systems such as Nexis and Dialog to discuss measures for protecting sensitive information. There are unconfirmed reports that defense and intelligence agencies have also visited banks, insurance, and credit firms to discuss the need to protect sensitive information citing NSDD 145 as authority. Although Nexis indexes and stores newspapers, Donald Latham, head of the NTISSC steering committee, expressed government concern about such databases in a Washington Post interview:

> "I'm very concerned about what people are doing--and not just the Soviets. If that means putting a monitor on Nexis-type systems, then I'm for it....The question is how do you do it technically without unnecessary interference."

On November 11, 1986 Diane Fountaine, Director for DOD's Information Systems, under Assistant Secretary of Defense Latham, spoke on the issue of regulating government and commercial data bases at an Information Industry Association convention in New York. Fountaine made public the definition of sensitive information contained in NTISSP 2 but offered no assurance that the definition applied only to government information systems. Fountaine was blunt:

> "I don't believe that the issue is whether or not we're going to protect information, I believe that the issue is what information we're going to protect both within the Federal Government, both within DOD and also within industry."

3. Protecting Systems and Limiting Information Dissemination

It is of critical importance to understand the ways in which defense agencies are attempting to protect information. Again, to allay public concern, Assistant Secretary of Defense Donald Latham has stated that NSDD 145 is only concerned with protecting communications and computer systems against unauthorized access.

In a letter to the President of the Information Industry Association on January 9, 1987 Latham wrote:

> "The essential thrust of the policy is to protect systems against unauthorized access. The policy is in no way intended to and will not affect authorized access to government or government-derived information. The releasability of information in response to requests submitted under the Freedom of Information Act, for instance, will not be affected by this policy." (emphasis original)

In fact much defense agency activity under NSDD 145 has been focused on developing procedural and technical means for protecting communications and computer systems. According to press accounts, government reports, and official testimony, the the Department of Defense and the National Security Agency's National Computer Center, acting pursuant to NSDD 145, are engaged in training, developing system security standards (e.g. Trusted Computer System Evaluation Criteria), contracting with private industry to develop secure phones, secure communications satellites, and data communications networks, working on introducing new encryption devices, and other such ventures. Some pose important policy issues as well--but are beyond the scope of our testimony today.

However, defense agencies are also exploring ways to limit the dissemination of unclassified sensitive information. Referring to the broad definition of sensitive information set forth in NTISSP 2, DOD's Fountaine stated at the Information Industry Association convention in New York last November:

> "This is the information that we intend, in certain respects, to at least protect in terms of dissemination".

> "We've got the categories of information and we need to be very careful about what we include in those categories and how we define the things we're actually going to protect, and control access to..." (emphasis supplied)

Today, DOD efforts to limit the dissemination of sensitive database information are focused on government and commercial databases which contain information of value to foreigners. In its Report on Soviet Acquisition of Military Significant Western Technology:An Update, the Defense Department made the following proposal to keep unclassified sensitive information in government and commercial databases from our adversaries:

> "One solution appears to be to thoroughly screen all candidate data base entries and keep sensitive information out of the public data bases or limit its availability to US and allied defense contractors. Unfortunately, this may also inhibit the United States' own national research effort by resisting the ready availability of such information."

4. Current Efforts to Control Data Bases

The Defense Department is now embarked on such a program to screen and limit information in government and commercial data bases sought by Soviets and other foreigners. Most disturbing is the effort by the government to control access to private computer databases. The government argument is simply that the Soviets do not have comparable databases and would benefit from subscribing. That is undoubtedly true in the same sense that the Soviets benefit from reading The New York Times or a congressional hearing record but it does not justify the imposition of government control over such public information sources.

For the moment the government seems to be seeking voluntary compliance from the information industry. However, if that is not forthcoming--as discussed in more detail below--the government appears ready to use various forms of coercion from the subtle (appeals to patriotism) to more explicit forms of mandatory controls, including:

--limiting the availability of data on line in government databases;

--placing selective limits on who may access government databases;

--monitoring who subscribes or seeks to use government databases and the nature of their inquiries;

--refusal to release or sell data in electronic form;

--licensing government database information subject to restrictions on access or further dissemination;

--contracting with private database companies to provide database services subject to restrictions on access or further dissemination;

--reclassifying data already disseminated to private data vendors;

--threatening commercial database firms with prosecution under the export control laws for failure to limit data dissemination.

This program to screen and limit information in government and commercial databases sought by Soviets and other foreigners was outlined by Diane Fountaine in November 1986 at the Information Industry Association convention. In outlining possible government measures, Fountaine acknowledged that a still secret Air Force study contains other proposals for limiting access by foreign nationals to sensitive information which are still under review. Although undertaken by the Airforce, the proposals "may apply across the Department (of Defense)."

Using the DOD's Defense Technical Information Center as an example, Fountaine suggested a number of restrictions based in part on the Air Force study:

> --"a one time review of the information that has built up in that data base over time--to insure that there is not militarily critical technology information that is not being protected or national security related, sensitive information..."
>
> --"some type of restriction based on bibliographic search so that people can not get to subject files unless they have the appropriate permissions to do so..."
>
> --"implement an automated system to detect any unusual use of that information that's provided in that system; I'm not sure we'll do that, but that is one of the recommendations..."
>
> --"provide a gateway from DTIC out to other commercial data bases; that one is a little tougher to do; but we may attempt to do that..."

With respect to commercial databases, Fountaine was less specific and more tentative:

> --"(W)e would like to begin to look at the commercial data bases and systematically try to assess what militarily critical information, if any, is in them."
>
> --"We'd like to do some automated analysis and have some automated tools for analyzing the information that is both in commercial information systems and also in the Federal Government system..."
>
> --"You (meaning the information industry) may not want to sell rights and accesses to all of your databases."
>
> --"You might want access and authentication to

> those data bases."
>
> --"You might want to know who's actually getting in them, and who's remotely accessing and control the long haul communications that are being used to access those systems."

VI. Legal Policy Issues and the Free Flow of Information

1. Commercial Data Bases

With respect to commercial databases, Fountaine's remarks suggest an emphasis on voluntary cooperation between government and industry to limit the dissemination of sensitive information. This is fully consistent with NSDD 145 requirements that government "encourage, advise, and where appropriate, assist the private sector" to protect sensitive information. It is also a recognition that the government's authority to impose content or access restrictions on private sector data vendors is extremely limited since overbroad restrictions would run afoul of the First Amendment. As Fountaine acknowledged:

> "There is also a long way to go in the interpretation on the legal side because most, of the law today does not deal specifically with information itself, it deals with more concrete things. We have legal controls in export and international law for things like systems, hardware, even some software. But for controlling legally the access to information it's not clear that the laws have been interpreted fully in that area."

Nevertheless, the government may succeed in limiting the free flow of unclassified information. However, Fountaine assured the IIA convention that the government will only impose necessary limits:

> "I don't believe there's any intent to restrict access within the Scientific and Technical information community to the extent that there

> is not adequate fertilization of thought within the community."

This is not reassuring. There are several reasons why government measures, from seeking voluntary cooperation to more mandatory measures, may severely limit the free flow of unclassified information now in the public domain.

Even government encouraging voluntary cooperation may adversely affect the dissemination of information. There is a fine line between encouragement and subtle coercion. Jack Simpson, President of the company which owns NEXIS, appeared on the same panel with Diane Fountaine at the Information Industry Association convention and described the visit by NSA and CIA to his company in terms of a "chilling effect." While government agents only inquired about sensitive data that might be available through NEXIS and whether the company had means for monitoring or limiting access, Simpson felt the agents delivered an implicit message that a refusal to cooperate would be unpatriotic and contrary to the national interest.

With respect to classified data, Executive Order 12356, the Reagan Administration Classification Order, authorizes the government to reclassify information already publicly disseminated. In a recent case, a court ruled in favor of the National Security Agency's reclassification of information which it had released but later retrieved from a library. Can the government reclassify information discovered in a commercial database?

Although government authority to control unclassified information already publicly disseminated is more tenuous, in the academic and scientific research context, the government has successfully threatened prosecution under the export control laws to limit dissemination of information to foreigners. The Air Force study may recommend that the government attempt to apply such controls to commercial databases.

Because of First Amendment constraints on regulating information in the private sector, the government is likely to focus its efforts to protect sensitive information while it is in the possession of the government. Commercial database companies may be required to limit access and dissemination of sensitive information based on contractual, licensing, or similar restrictions.

2. Government Data Bases

The government may limit the disclosure and dissemination of information classified pursuant to executive order. It may also seek to protect categories of information exempt from disclosure by statute (e.g. trade secrets, Privacy Act Records, etc.) The problem is that under NSDD 145, the government is attempting to restrict the flow of unclassified sensitive information under a definition (NTISSP 2) which greatly exceeds all current statutory limits on the disclosure of information.

The definition on its face covers extensive amounts of information in the public domain. Placing limits on the dissemination of this information would appear to violate the Freedom of Information Act and other statutes which provide for the dissemination of government information.

A critical issue that requires examination is whether the government may lawfully impose "licensing" restrictions on government data in electronic form consistent with the Freedom of Information Act. The government temptation to attempt to license electronic data is considerable. First, government must find a way to control information dissemination by private sector vendors who are not subject to government contractor restrictions or who disseminate sensitive information beyond the scope of the export control laws. It also stems from the government-held belief that data in electronic form poses more of a threat to national security than paper records.

Under NSDD 145 one definition of sensitive information is information which "even if unclassified in isolation...can reveal highly classified and other sensitive information when taken in aggregate." Electronic data is easily assessed, searched, and retrieved. Therefore, according to the government, it makes it easier for our nation's adversaries or other foreigners to aggregate and thereby acquire sensitive data more readily. As the update report on Soviet acquisition of western technology states:

> "(T)he individual abstracts or references in government and commercial data bases are unclassified, but some information, taken in the aggregate, may reveal sensitive information concerning U.S. strategic capabilities and vulnerabilities...The growing use of electronic data bases has provided the Soviets with an even more efficient means of identifying and procuring such unclassified technical information."

Presently the government is experimenting with licensing schemes to restrict information in providing databases services to the private sector. For example, in exchange for "lease /use of the EDB/NSA" files of the Department of Energy, the Department of Commerce is attempting to limit through contractual arrangement the "sale of database services to U.S. organizations deemed likely to transfer the information to any foreign third party" and require users "on a semi-annual basis...(to) provide NTIS (National Technical Information Service) with the names and addresses (domestic and foreign) of the users of DOE data files. Recently, it was revealed that the National Aeronautics and Space Administration has been keeping a list of information companies who are not to receive subscriptions to unclassified government documents on the grounds that they are thought to have foreign clients (e.g. NASA "No No" List).

The government may claim the authority to impose such restrictions based on case law which suggests that the public is not entitled to data in electronic form if a hard copy is available. See DC v. Matthews, 542 F. 2d 1116 (9th Cir. 1976); Dismukes v. Interior, 603 F. Supp. 760 (D.D.C. 1984). If the public is not entitled to electronically stored copies of public information, the government might make such data available subject to licensing agreements that restrict electronic data dissemination. Because more government data is being computerized and is more valuable to the public in electronic form, there is a significant danger of government licensing schemes or other related mechanisms (e.g. the "gateways" to government databases proposed by Fountaine to the IIA) which could severely impair the public's right to know in the computer era. In effect, the government's discretion to provide electronic versus hard copy data may give the government what amounts to a *de facto* copyright over public information in electronic form. See Electronic

Collection and Dissemination of Information By Federal Agencies: A Policy Overview (Rep't 28, Committee Government Operations, No. 99-560, April 29, 1986)

It should also be noted that the government increasingly is contracting with private companies to provide data services to the government. It fact it continues to explore privatization of the National Technical Information System. It could attempt to impose dissemination restrictions as part of these contractual arrangements.

VII. Impact on Scientific Inquiry and Competitiveness

A major policy issue raised by NSDD 145 information controls is their impact on scientific inquiry and competitiveness. The free flow of information sustains our democracy and fosters scientific, technological and economic advancement. There are a number of reports, including the soon to be released study by the National Academy of Sciences on the Impact of National Security Controls on International Technology Transfers, which indicate that:

-- Information controls may hinder our own national research efforts;

-- Restrictions on technology may adversely affect our lead over other countries in various advanced technological markets;

-- Both the costs of communications and computer security to meet government specifications and limitations on information services (data and customers) may adversely impact on the competitiveness of our growing information industry;

-- The costs of information security, including limits on the dissemination of sensitive information, outweigh the benefits since the policy is ineffective as our adversaries are able to obtain the information from other sources.

VIII. Military Control On Open Government

NSDD 145 gives the Department of Defense and the National Security Agency the central role in protecting government and private sector communications and computer systems which disseminate or store sensitive information. This poses a number of civil liberties issues.

1. Free Flow of Information

From the perspective of maintaining open government, it is unwise to put the military in control of civilian and private sector information systems. As Representative Jack Brooks, Chairman of the House Government Operations Committee, warned in testimony before a House Subcommittee:

> "One of the benefits of a full and open society is the rich exchange of ideas and knowledge unfettered by government intervention and red tape. The successes of our scientific, technical, and medical community have been based upon the free exchange of data and information. Since it is the natural tendency of DOD to classify everything, it would be impossible for the Department to strike an objective balance between the need to safeguard information and, the need to maintain the free exchange of information."

Pursuant to NTISSP 2, each agency is to determine on its own what information is sensitive and requires protection. However, if the government-wide effort is coordinated by the military, the governmental emphasis on "national security" will engender on the part of government agencies a tendency to err on the side of restricting information as agencies do today in overclassifying information.

Although defense agencies may only encourage the cooperation of the private sector, military agencies may have a "chilling effect" on commercial database firms. Firms may believe that a failure to cooperate with government requests to limit information dissemination or access implies an unwillingness on their part to protect "national security" and other government interests.

2. Privacy

In attempting to protect the secrecy of sensitive unclassified information in civilian agencies, defense agencies may recommend the adoption of procedures used to protect classified information that could adversely impact on privacy. More employees may become subject to extensive background investigations. Civilian agencies may be encouraged to employ new authentication devices and use software which monitors who accesses computers and how data is used.

3. Intelligence Surveillance

Under President Reagan's Executive Order on Intelligence, E.O. 12333, the National Security Agency and Central Intelligence Agency are prohibited from engaging in foreign counterintelligence or domestic security surveillance of United States citizens or organizations in the United States. However, pursuant to NSDD 145, NSA and CIA agencies are monitoring commercial database firms. They are attempting to identify firms which store or disseminate unclassified sensitive information, determine who uses these systems and how, and assess the security posture of private sector entities. This obviously could lead to the creation of files or "lists" of private firms who are cooperating in protecting national security and those who are not. These new intelligence activities appear inconsistent with the restrictions in Executive Order 12333 which governs intelligence activities by defense and foreign intelligence agencies of the United States and which largely limit their domestic intelligence role. As the House Government Operations Committee observed in its August 1986 report:

> "(NSDD 145) gave the NSA the authority to use its considerable foreign intelligence expertise within this country. This is particularly troubling since NSA was not created by the Congress, but by a secret presidential directive and it has, on occasion improperly targeted American citizens for surveillance."

There are good reasons for current limitations and why we should worry about whether they are being eroded by NSDD 145. NSA operates outside the normal accountability channels which control other agencies of government. It has no legislated charter. Its existence was not acknowledged until 1962. No Director of NSA appeared in open session of Congress until 1975--and then only to answer to a series of programs of illegal acquisition of international cables and "watchlisting" and interception of the communications of anti-war and civil rights activists. Because of the "States Secrets Privilege," civil suits against NSA for unauthorized surveillance routinely have been dismissed to protect its super-secret surveillance capabilities.

IX. H.R. 145 and Issues For Resolution:

We have reviewed H.R. 145. As we interpret the legislation, it is designed to respond to two critical issues posed by NSDD

145. First, it would attempt to reestablish civilian control over unclassified information systems by vesting authority in the Department of Commerce and The National Bureau of Standards. Second, we interpret the legislation to provide that the Commerce Department and NBS may establish procedures for protecting systems which communicate or store unclassified sensitive information as defined in the statute but may not limit access to unclassified sensitive information.

We endorse these objectives. We do not believe that DOD or NSA or the intelligence community are appropriate agencies to control communications and computer security in the civilian or private sector. Their tendency is to keep secrets and they have amply demonstrated that they do not weigh privacy and open government in the balance or if they do, they always strike the balance in favor of secrecy.

Moreover, we do not believe foreign intelligence agencies should be monitoring or surveilling private companies in the United States to determine which companies or executives are taking "appropriate" security measures or disseminating public information to the "wrong" people or "No No" list. Intelligence agencies may intimidate companies or have a "chilling effect" on their information dissemination practices. Companies will not want to be on a list or in a file of "uncooperative" companies who lack proper consideration for national security.

More importantly, we do not believe military or civilian agencies should be restricting access to public information they term "sensitive." If it is information which endangers national security, it should be classified. If it is protected under another statute--such as proprietary data--it should be protected. But if it is not protected from disclosure by statute, it should be public. In essence, we question the wisdom or necessity of creating any category of sensitive information in law. It constitutes a dangerous, slippery slope. Should there be such a definition in H.R. 145?

There is an assumption underlying government efforts to restrict database information that information is more sensitive, dangerous, or more subject to regulation if it is in "electronic form." Such a policy assumption can only wreak havoc on open information policy in this age of electronic information. First Amendment rights must not be diminished because information is in electronic form or communicated over new electronic media.

Congress needs to consider other issues in the process of legislating in this area. It is not clear how many issues there are here but at least the following need to be addressed.
It should look carefully at the economic cost of security measures and how those costs impact on the emerging information industry. It should learn the competititive impact of any restrictions on data which may result from regulation, such as the loss of data service markets to foreign competitors. It should also make an effort to determine in this information-linked world whether efforts to restrict access can be effective. To block access to Soviets and others may only hinder our own citizens' access to information as foreigners turn to other ready sources for the same information. In some cases, regulation of information may also injure our own technological growth rather

than slow the advance of others.

We also have some specific questions about H.R. 145. Is there a need for a statutory definition of sensitive information? Isn't it sufficient to define protected information as classified or unclassified information protected from disclosure under other statutes?

Is H.R. 145 drafted to ensure that Commerce or the NBS may not attempt to limit access to information in systems containing protectable information?

Does H.R. 145 need to be drafted to ensure that any protective measures are consistent with the Freedom of Information Act?

Even if it is, does this go far enough? There may be a need to clarify citizen access to electronic data under the FOIA to avoid government having the discretion to grant access to electronic records only on condition that purchasers or users limit further dissemination of information.

There is also a need to ensure that government contracts with private companies to provide database services to the government which contain unclassified information will not contain provisions which limit access or place other restrictions on dissemination (e.g. requiring companies to monitor who accesses systems or what kinds of queries are being made).

Congress should explore these issues with care. In March, a number of organizations and experts are holding a consultation on the issue here in Washington. These and other issues will be discussed in detail. We hope you or your staff will attend.

X. Conclusion

Mr. Chairman. Again thank you for this opportunity to testify here today. We believe that H.R. 145 is extremely important legislation and we look forward to working with you, the members of the Committee, and your staff on this proposal. We would be more than pleased to provide additional information or assistance at your request.

IEEE **WASHINGTON OFFICE**
THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
1111 19th STREET, N.W. WASHINGTON, DC 20036-3690, U.S.A. TELEPHONE (202) 785-0017

STATEMENT OF

JOHN M. RICHARDSON

on behalf of
THE COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY
of the
INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
on
THE COMPUTER SECURITY ACT OF 1987

Before the Committee on Science, Space & Technology
Subcommittee on Science, Research and Technology
Subcommittee on Transportation, Aviation and Materials
United States House of Representatives

February 26, 1987

IEEE WASHINGTON OFFICE
THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
1111 19th STREET, N.W. WASHINGTON, DC 20036-3690, U.S.A. TELEPHONE (202) 785-0017

STATEMENT OF

JOHN M. RICHARDSON

on behalf of
THE COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY
of the
INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
on
THE COMPUTER SECURITY ACT OF 1987

Before the Committee on Science, Space & Technology
Subcommittee on Science, Research and Technology
Subcommittee on Transportation, Aviation and Materials
United States House of Representatives

February 26, 1987

Chairman Walgren and Chairman McCurdy, my name is John M. Richardson. I am Chairman of the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers, Inc. (IEEE). My statement is presented on behalf of that committee. The IEEE is the world's largest engineering society, with nearly 280,000 members worldwide, 229,000 of whom live and work in the United States. The IEEE Committee on Communications and Information Policy (CCIP) is vested with authority to develop the Institute's communications and information policy; and, once that policy is adopted by the Institute, our committee is one of the major mechanisms by which the policy is voiced in public.

We appreciate this opportunity to present our views on H.R. 145, the "Computer Security Act of 1987." This bill is closely related to National Security Decision Directive (NSDD) 145, entitled "National Policy on Telecommunications and Automated Information Systems Security" (September 17, 1984), and to

National Telecommunications and Information Systems Security Policy (NTISSP) No. 2, entitled "National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems" (October 29, 1986). All three documents address the issue of sensitive, but unclassified, information in Federal computer systems, but from different perspectives. NSDD 145 limits itself to information, the loss of which could adversely affect the national security interest; it admits both government and nongovernment information into this class. NTISSP 2 does not explicitly state whether it deals with government information only, but in any case it broadens sensitive, but unclassified, information to other Federal Government interests as well as national security. Both NSDD 145 and NTISSP 2 undertake to provide guidance to all agencies of the Executive Branch from the National Manager for Telecommunications Security and Automated Information Systems Security, that is, the Director, National Security Agency. H.R. 145 would separate the protection of classified national security information from that of sensitive, but unclassified, information and would give a civilian agency responsibilities to assist other civilian agencies.

To anticipate the main points of my statement, first we oppose government categorization and protection of nongovernment information. Second, we endorse the intent of H.R. 145 that a civilian agency rather than a defense agency should assist other civilian agencies and the private sector in the protection of computer systems. Third, we believe that NTISSP 2 should be rescinded as too broad, and that uniform and workable guidelines should be developed to limit the amount of government information designated as sensitive and the associated abridgment of access to it. Fourth, we recommend that studies continue to ascertain the balance between all the costs and benefits of such protection. It will be a major contribution of the Congress to make clear just what the Federal government role is and how responsibilities for implementing this role are assigned among agencies.

IEEE cares about these matters because many of its members have expertise in the techniques of such protection. More importantly, these matters affect access to government information by our profession. Government actions may also have great influence on protection policies and practices ultimately required of or adopted by the private sector, in which most of our members are employed. In such a climate, IEEE sees the free flow of scientific and technical information as an important underpinning of the robustness of U.S. technology and our economy.

Let me recall points I made in previous testimony on June 27, 1985. There are three distinct aspects of the subject: (1) classified information; (2) other sensitive, but unclassified, government or government-derived information; and (3) sensitive nongovernment information. Classified information is protected by existing law and Executive Order and is not at issue. The attempt of NSDD 145 to deal with sensitive nongovernment information is ill-conceived and the directive should be modified accordingly. In my previous testimony I said I had no comment on sensitive, unclassified government information, and that it might be protected as the government sees fit. I would like to revise that position in this statement to point out certain dangers of trying to protect too wide a range of the government's own information.

Five important issues seem to us to require attention. These issues are posed as questions, with ensuing discussion.

1. Is there really such a thing as "sensitive, but unclassified information, the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal government interests" [NTISSP 2]?

We submit that there is no such thing as sensitive nongovernment information that the government should be concerned with. We do agree that there is government information of such a nature, like social security and tax data, just as there is personal and proprietary information that has come to enjoy protection under law and custom. We further agree that the determination of what government information is sensitive should be decentralized in some way, so those who are closest to its significance can assess the consequences of its compromise. But these classifiers should not enjoy the unconstrained powers now granted them by NTISSP 2; they should follow guidelines developed from careful rulemaking.

2. How should we approach its protection?

NSDD 145, NTISSP 2, and H.R. 145 provide that government systems handling such information shall be protected. In principle, this approach is necessarily analogous to the one used for classified material: namely, information is first reviewed, classified, and marked; then it is stored, transmitted, and processed only within secure systems. In practice, this approach would almost surely break down for sensitive, but unclassified, government information because so far it is neither well characterized nor well marked. If unmarked sensitive material gets into an unprotected channel, it may be compromised. If all information, sensitive or not, is handled in protected channels, we incur the cost of an unnecessarily large protected system. More importantly, we also inevitably limit access to the system by erecting barriers to its use, not only for those we wish to impede, but in some degree for those we do not. These points are clear from the following simple diagram:

Information	Systems	
	Protected	Unprotected
Sensitive	Secure	Compromised
Insensitive	Expensive, inaccessible	Inexpensive, accessible

3. How can the costs of protecting too much information and abridging access to it be avoided?

The diagram shows that the more you cover the less access you allow. Therefore, the class of sensitive government information should be defined as narrowly and precisely as possible so that protected systems can be matched to it without incurring the expense and the abridgment of access that would accompany the inclusion of insensitive material in the protected system. This is the classified information problem all over again. Too little quantification of the consequences of compromise of this kind of information has occurred. Too little analysis of the direct costs of the protection itself has been done, and who should bear them. Likewise, too little analysis of the indirect costs of abridged access has been done. For example, IEEE deems the unabridged dissemination of unclassified scientific and technical information crucial for the continued advancement of U.S. industry, and we oppose restraints on its exchange.

4. Are there adequate guidelines for a workable definition of sensitive, but unclassified, government information and for identification of government systems handling this information and thus needing protection?

NTISSP 2 defines sensitive, but unclassified, information as follows:

> Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

In my 1985 testimony I urged "extreme restraint" in designating categories of sensitive information. This definition is not extreme restraint. Furthermore, it does not explicitly limit itself to government information, so we face uncertainty as to how far the policies of NTISSP 2 may reach to nongovernment information, with repressive effect.

The definition in H.R. 145 is almost equally broad, without citing specific fields. We believe that both definitions are overly broad. They are not operational, in the sense of telling you what you have to do in order to determine whether information is sensitive. Consequently, both would pose almost insuperable difficulties in implementation because of the great variety and pervasiveness of information flowing within our society. The boundaries of any such categories are inevitably diffuse and cannot be characterized with precision. The result would be reduced to the arbitrary and subjective opinion of particular administrators. Thus, there is a risk of casting too wide a net as to both information and systems in carrying out NTISSIP 2 and H.R. 145.

5. Should there be some separation of responsibilities for determining and protecting government information affecting the national security and that affecting other Federal government interests?

There has been considerable confusion in the private sector concerning the respective jurisdictions of the Department of Defense and the National Bureau of Standards in the development and use of information security technology. We favor a clean division of responsibilities. Let the Defense agencies classify and protect all government information the compromise of which would pose grave danger to the national security. Let the civilian agencies determine government information the compromise of which would adversely affect other Federal government interests and protect the systems that handle it.

Having made these points, we can now crystallize our views on H.R. 145.

1. H.R. 145 is needed to reaffirm and clarify that one mission of the National Bureau of Standards is to develop standards, guidelines, and associated methods and techniques for computer systems and to assist the civilian agencies and the private sector in this regard. Such a separation is needed between national security concerns and non-national security concerns with respect to government information to avoid applying the biases of national security to other areas.

2. H.R. 145 and NTISSP 2 both fail to provide workable guidelines for agency heads to identify and designate sensitive, but unclassified government information. NTISSP 2 should be rescinded and the Congress should require that practical and uniform criteria for this process be publically developed and adopted.

3. H.R. 145 should also provide for an assessment of the long-term benefits versus costs, both direct and indirect, of determining sensitive, but unclassified, government information and protecting the government systems that handle it. Such a study would be a valuable precursor to the enactment of legislation.

Chairman Walgren, Chairman McCurdy and Members, thank you for your attention to my statement. I will be happy to address any questions you may wish to put.

BIOGRAPHICAL SKETCH

JOHN M. RICHARDSON
Principal Staff Officer
Energy Engineering Board
National Academy of Sciences-National Research Council

John M. Richardson is a Principal Staff Officer with the Energy Engineering Board of the National Research Council of the National Academy of Sciences. He has been responsible for the staff direction of studies of the solar power satellite concept, electronic mail, electromagnetic pulse effects, and magnetic fusion.

He was previously Chief Scientist of the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, from March 1978 to October 1979. From the date of its establishment in 1970 to 1978 he served variously as Deputy Director, Acting Director, and Director of the Office of Telecommunications, one of the predecessor organizations of NTIA.

His prior employment includes service as Executive Secretary of the Committee on Telecommunications of the National Academy of Engineering while that committee performed studies for President Johnson's Task Force on Communications Policy in 1968-69. At the National Bureau of Standards, Boulder, Colorado, he served as Deputy Director for Radio Standards of the Institute for Basic Standards from 1962 to 1967.

He also served on the staff of the Assistant Secretary of Commerce for Science and Technology and, in this capacity, was instrumental in the establishment of the Office of Telecommunications in 1970.

Dr. Richardson, who has published numerous papers on technical specialities and on more general aspects of communications technology and public policy, received the Department of Commerce Gold Medal Award for Exceptional Service in 1964. He has frequently represented the United States at the Organization for Economic Cooperation and Development.

Dr. Richardson received his B.A. degree from the University of Colorado in 1942 and the M.A. and Ph.D. degrees in physics from Harvard University in 1947 and 1951, respectively. In 1966-67, he returned to Harvard to spend a sabbatical year at the John F. Kennedy School of Government.

APPENDIX

STATEMENT FROM LEE NEUWIRTH OF CYLINK ON HR145

I appreciate the opportunity to present to you my ideas on a number of subjects with important connection to HR 145, as well as some thoughts on the bill itself.

My name is Lee Neuwirth, I have a B.S.E. from Princeton in Engineering (1955), an M.A, in Applied Mathematics from Columbia (1957) and a Ph.D. from Princeton in Pure Mathematics (1959).

In 1961 I joined the Communications Research Division of the Institute for Defense Analyses (IDA). I worked as a member of the Technical Staff until 1965 when I became Deputy Director. In 1977 I was appointed Director. I served in that post until 1985 when I joined CYLINK.

At CRD we worked almost exclusively on problems of communications security. Over my 24 years of contributions there I wrote much and learned many lessons, not the least of which was that cryptology is a weapon of war, very powerful and extremely important to any enterprise in which concealing information is essential. Since I left CRD and entered the commercial world I find that concerns there are almost the same, albeit (at the moment unfortunately) less urgent. The threats are the same, the protection needed comparable in scope if not in degree. In fact the potential evesdropper may in some cases be the same person!

The views expressed here are my own, modulated by my company's business concerns.

CYLINK

Founded in 1984 under the name Omnet, we were funded in 1985 by the Pittway Corporation and a venture capital company. We changed our name soon after to CYLINK.

We design, manufacture and sell encryption equipment, with special emphasis on key management. Our main office is at 920 W. Fremont Avenue in Sunnyvale, California 94087, (408-735-5800). My office is in Suite B-19, 601 Ewing Street, Princeton, New Jersey 08540, (609-683-1150).

Our company is growing and currently employs about 27 people.

We currently have a product line including:

A high speed link encryptor called the CIDEC-HS which

1

is 1027 endorsed and handles data at rates up to 7 megabits.

A medium speed link encryptor called the CIDEC-MS which has been submitted for 1027 endorsement and handles data at rates up to 112 kilobits.

A key management chip which exponentiates 1028 bit numbers in under a second.

A facsimile encryptor, the FAXLOK.

In addition we have under development a high speed encryptor as part of the CCEP, and will be developing under CCEP a very high speed encryptor as well.

We are in the final stages of developing a fully automated single board encryptor for a microwave radio company and an intelligent channel service unit and network security diagnostic system for a Fortune 500 company.

NSA/CYLINK interactions

We applied for 1027 approval of our CIDEC-HS product in late '85 and received the endorsement number 00000025 in early

'86. We had many technical and administrative interchanges with NSA over those months and found our contacts to be cooperative and cordial as well as careful. They were responsive to our concerns, although often unyielding in their positions on requirements. As far as we can tell they have made every effort to be consistent in both their reading of the 1027 technical documents and their interpretation for physical devices. They demonstrated high technical competence, and devotion to task which resulted in a better documented, stronger product for us, at a modest increase in cost. In addition they recognized the need for flexibility from a commercial point of view, and permitted the inclusion in our product of a "commercial" mode in which their requirements (for example for key management) were relaxed. We have been comfortable with this arrangement, anticipate no serious problems with our recent submittal and may submit still another application later this year.

DES

Because of all the recent furor concerning the DES algorithm (DEA) we would like to state our opinions on DEA in particular, and other algorithms in general.

The DEA has not been shown by anyone (to my knowledge) to have subtle or overt weaknesses. So far as I know exhaustion is the only feasible attack, with an outside chance of using the complementary property to gain a factor of 2. In any case the algorithm is sound and I believe mutterings of a trapdoor are untrue. I have seen zero evidence of a hidden weakness.

Having said this I must add; all algorithms age. One never learns anything good about the strength of an algorithm, no one ever discovers the algorithm is stronger than expected. DES will become insecure someday, as did our W.W. II devices, as will any crypto machine. The question is when? The present course is inevitable, triple encryption with DES is awkward and inefficient except for special cases. DES will have to be replaced someday.

I see no reason to make a crypto algorithm public (even making DES public did not eliminate suspicions). Algorithms are definitely safer when secret. Every algorithm becomes weaker in time;.why hasten that process?

My company and I have much greater confidence in the NSA crypto logic designers then in those of the outside world. I do not believe NSA wants to read the commercial traffic of U.S. companies, they have many priorities and that's not one of them. On the other hand they do have as a priority seeing U.S. companies and individuals as well as the U.S. government secure their communications.

CCEP

The CCEP seems to be a tough program to get into, it took CYLINK about a year. Much information was required, many discussions took place. We are proud to be a part of the program, and believe it should be hard to get into. As stated earlier, cryptology is a weapon, it should be handled carefully and those given access to the powerful encryption machines the government can make available should be highly qualified, trustworthy, and of unequivocal and unquestioned loyalty to the United States.

We have heard criticisms that the algorithms supplied will not be made public. We see no problems in not knowing algorithms' details. We trust the government, and find it a contradiction to believe there are known weaknesses in the new algorithms we will be supplied with and that the same algorithms will be used to secure sensitive government material. So we believe the algorithms to be strong.

We have heard it stated that since the government supplies keying material, they will be able to read the traffic. For the key management system we are being supplied with this is certainly not the case.

We have heard the complaint that the algorithms are not upward compatible, that different algorithms are used for different speeds. Even CYLINK's own products, (and those of competitors) are not upward compatible in that sense. We use 64 bit output feedback at high speeds and 1-bit cipher feedback at lower speeds in our DES products. This is a commercial necessity. Self-synchronizing devices are much more desirable than those having a resynching protocol. However self synching is not available at high speeds because no chip can run fast enough at present. In addition some algorithms are fast, but not suitable for microprocessor implementation. These and other factors make algorithm diversity necessary. Incidentally this diversity also adds security, by not putting all the eggs in one basket.

STANDARDS

Standards in the classic sense, where the time frames involved may be dozens of years are not consistent with the dynamic nature of cryptology. Technology and mathematical breakthroughs constantly threaten security and must be continually reevaluated. Planning for the future is all well and good, but you can't plan on an as yet unenunciated mathematical result. Instead, one must be prepared in this business to react quickly and decisively in the face of research results.

SECURITY

We strongly believe that the ability of the private citizen, corporation or government to keep some things private is a requirement for the preservation of democracy. The means to this end is available, the will to execute these protections seems present. What is needed now are funds to put such protection as is now available in place.

ENCRYPTION

We believe encryption has a great future, as do authentication and verification. In the electronification of America the protections we now enjoy must not be sacrificed. Their preservation is through electronics.

The bill confuses us; we believe it will confuse our customers and create chaos in the market place. We have expressed our concerns below:

A.) What is wrong with what is happening now? We see an orderly, sensible, effective movement to making better security equipment available to the commercial market through (for example) the CCEP.

B.) We have experienced no problems of consequence in developing a product, acceptable in the marketplace with minimal added cost due to 1027. From all we have seen in the CCEP we anticipate a still better product, again with minimal effect on cost from NSA requirements.

C.) Who's in charge under HR145? Now NSA processes applications, has the algorithms, is responsible for evaluation, grants approval of variants, issues an endorsement and supplies certain materials for qualified operators of commercial equipment. The proposed legislation spreads all this over two agencies over the lifetime of the product. It has been my experience that divided responsibility for security in general results in diminished security. This is due to leakage at the seams as well as to confused or inappropriate assignments.

D.) A vendor will presumably still have the option under HR145 of manufacturing a product for NSA approval (for example for securing DOD UNSR links). This presents a serious problem in product definition. The niches for security equipment are not large now, if they are further narrowed by deciding on development of a product for NBS or NSA certification or developing both, the economic incentives for the business are considerably reduced, the number of product variants proliferates, and confusion enters.

E.) Which communications links in a center or network of centers would NBS be responsible for approving security or setting security standards for and for which would NSA be responsible? Would White Sands proving ground or Yuma negotiate with NBS over UNSR links? What about the Coast Guard or a defense contractor or subcontractor's links? Having two agencies responsible for data encryption and computer security seems like asking for trouble.

F.) We have seen no military interference with our products for the commercial market, and not a whisper of future interference, only suggestions for improving the product, including its marketability.

G.) NSA has already incorporated ANSI X9.17 and X9.9 standards in directives to us for inclusion in our box. This seems to us an excellent interface and path along which such standards will propagate.

SUGGESTION

A good thing might be to encourage the use of encryption and security products with a tax incentive or direct appropriation. At present we see heel dragging in complying with various governmental directives requiring protection of information.

Thank you,

Respectfully Submitted by
Lee Neuwirth
Vice President Product Planning

Statement of the

American Library Association

for the

Subcommittee on Transportation, Aviation and Materials

House Committee on Science, Space and Technology

on
HR 145, the Computer Security Act of 1987

March 18, 1987

This statement is submitted on behalf of the American Library Association (ALA), a nonprofit educational organization of nearly 44,000 librarians, library trustees, and friends of libraries. We appreciate the opportunity to present our views on HR 145, the Computer Security Act of 1987, and related issues of security and access in regard to U. S. government databases.

Libraries---and the databases of printed or computer-stored information which support them---are the most durable and enduring of all information institutions in this country. They are central to an informed citizenry from childhood through the highest research and intellectual endeavors of maturity. They bear the honorable burden of providing the first line of defense for intellectual freedom and the right of citizens to secure any information useful to them. Our Association is especially vigilant concerning information which is generated by our government and paid for by its citizens.

We would like to address two problems, which, at first glance, might seem to be in conflict with each other: the security of our federal libraries and databases, and the provision of the broadest possible access to these services. In our view, security and access are two sides of the same coin. When people enter a hospital they demand that:

- the facility be physically safe,
- that its systems and controlled materials are made secure,
- that their privacy be maintained, and
- that the staff include well-trained professionals.

It is these factors which preserve the integrity of the system. In no way do they impede, in fact they encourage, public access. Information systems (and libraries) demand the same kind of management in order that their integrity can be preserved and access to quality services can be maintained.

Thus, we share your concern that databases developed by the government, and used by the citizens, be physically secure, free from misuse or fraud, safe from unauthorized modification or loss of information; and that the privacy of citizens about whom information is deposited in some of the databases, be protected.

The American Library Association congratulates the Subcommittee for bringing this important problem into focus, and for forming a plan whereby national standards for security can be promulgated, and dissemination and training can take place. We support HR 145 because the bill assigns to the National Bureau of Standards (NBS), a non-regulatory agency, the task of providing a computer standards program which would assure government-wide computer security. NBS is the nation's single governmental metrological laboratory which was established for the express purpose of promoting the prosperity and growth of American industry and commerce. Because it has no partisan or regulatory axes to grind, NBS is eminently suited to develop important, realistic computer security standards to assure the consistent integrity and validity of information electronically generated by the government.

The history of NBS's Federal Information Processing Standards (FIPS) Program demonstrates that the Bureau can and does provide an open, dispassionate, scientific environment which is necessary for development and implementation of realistic information standards for the information community. Indeed, industry, academe and federal agencies work together to assure that FIPS standards are accepted and applied by the widest possible groups.

HR 145 is entirely consistent with the President's policy on this issue as promulgated in the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," issued on December 12, 1985, which directs the Secretary of Commerce to:

> o Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology...
>
> o Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;
>
> o Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;
>
> o Develop, in consultation with the Secretary of State and the Director, OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities...

However, there are counter forces operating which could nullify the positive effects of HR 145. ALA is concerned about recent efforts of the Administration to vest the Department of Defense and certain intelligence agencies with authority to control and limit access to virtually the entire information universe, including information resources maintained by or available from domestic agencies of the federal government (for example, the information resources of the National Technical Information Service), and the information resources available from such commercial database vendors as Mead Data and Dialog. These databases contain information available in many public libraries and in most federal libraries. The Association believes that HR 145 is a necessary first step to blunt these efforts by vesting the authority to determine the parameters of computer security for domestic federal information resources in an impartial, scientific civilian agency such as NBS.

For some years now, ALA has viewed with increasing alarm the Administration's frequent, and frequently inconsistent, edicts designed to restrict or to cut off access to unclassified information, especially unclassified technical or scientific information, it felt might "adversely affect national security or other Federal Government interests." We believe one such recent edict, namely National Telecommunications and Information systems Security Policy (NTISSP) No. 2, "National Policy on Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems" (29 October 1986), would permit federal agencies to keep secret almost anything they choose. NTISSP No. 2 defines "sensitive, but unclassified information" as:

> ...information the disclosure, loss, misuse, alteration, or destruction of which would adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

Thereafter, the Policy directs the heads of federal government departments and agencies to determine "what information is sensitive, but unclassified to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems."

The framework for the implementation of NTISSP No. 2 appears to be already in place through National Security Decision Directive 145, signed by President Reagan on September 17, 1984. As the Foreword to NTISSP No. 2 notes: "NSDD-145...provides policy and direction for systems protection and safeguards telecommunications and automated information systems that process or communicate sensitive but unclassified information." The American Library Association is opposed to any policy intended to deny ready and equal access to unclassified government information by U.S. citizens. We find it puzzling that on one hand the Administration is worried about people in this country obtaining unclassified but potentially sensitive information, but they are apparently not at all concerned about foreign companies having control of our databases and federal libraries.

ALA is persuaded that implementation of NTISSP No. 2 will construct a formidable barrier to the free flow of information and to open government, and will surely erode further Congress' duly constituted authority in this vital area. Therefore, on January 21 of this year, during the Association's Midwinter Meeting in Chicago, ALA's Council passed a resolution which states that NTISSP No. 2 is in conflict with three of the Association's established policies. The resolution states that ALA will seek to have NTISSP No. 2 repealed or rescinded; will cooperate with other organizations to challenge its implementation; and will request the Freedom to Read Foundation to be alert to an opportunity to challenge its legality. A copy of the resolution is attached to our testimony. ALA believes that enactment of HR 145 would afford an appropriate opportunity to request that NTISSP No. 2 be rescinded. We urge Congress to press for its rescission. On June 27, 1985, in testimony before this Subcommittee, the Chairman of the House Government Operations Committee stated that he believed NSDD 145 to be:

> One of the most ill-advised and potentially troublesome directives ever issued by a President. It seeks to vest in the Department of Defense...the authority to...govern the access to and processing of all computerized information which it deems to be critical to the national security of the United States. This would include not only classified information but any other information within... civilian agencies which the Department considers 'sensitive.' The Directive would also give DOD the power to influence the collection, processing and dissemination of information in the private sector ...Since it is left up to the Department to define what is in the interest of national security, virtually any information system located in the civilian agencies or in the private sector would fall under its domain...This Directive...was drafted in a manner which usurps Congress's role in setting national policy...The corridors of the Pentagon and the offices of the...White House are not places in which national policy should be established...The Directive is in conflict with existing statutes which assign to the Office of Management and Budget, the Department of Commerce and the General Services Administration the sole responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security. In issuing NSDD 145 the President ignored these statutory authorities...The President does not have the authority under our constitutional form of government to unilaterally revise existing standards.

ALA agrees with Chairman Brooks' assessment of the illegality of NSDD 145. We would have quarreled with the intent of NSDD 145 much sooner. Unfortunately, we did not know about it because the White House did not announce its existence for almost a year. In any case, we urge this Subcommittee to do whatever it takes to assure that NSDD 145 will not become further embedded in national information policies.

ALA finds it incongruous that the Administration is trying to restrict foreign access to unclassified scientific, technological and economic databases, and yet permits U. S. subsidiaries of foreign firms to take over and operate federal library and information services which provide access to this same information. In a February 9 New York Times article (attached), Members of Congress were quoted as concerned that current government policies on providing foreign access to sensitive scientific and technical information are inconsistent. The article pointed out that one foreign-owned company that has been awarded several military database contracts is C. L. Systems Inc., a wholly owned subsidiary of TBG Inc., which is based in the Netherlands Antilles, and privately owned by a Swiss industrialist. It was recently announced that this same firm has won a contract to provide an integrated library system for the White House Library. The library literature also reports that C. L. Systems Inc. has signed a contract for an automation project with the National Library of China, one of the largest libraries in the world, which serves the business and government communities of Beijing.

Still another company mentioned in the article, Aspen Systems Corporation, which is owned by Wolters Samson, a Dutch corporation, appears to be the successful bidder on the A-76 contract to operate the Library and Information Services Division of the National Oceanic and Atmospheric Administration in Rockville, Maryland, one of the government's major scientific and technical libraries. In addition, Aspen Systems currently operates the library of the Department of Housing and Urban Development, which we understand includes the agency's Freedom of Information Act unit and the agency access point to precisely those external databases the Administration is trying to shield from foreign access. It should be noted that libraries within federal agencies also must have access to internal databases if they are to perform the basic function for which they exist.

There are a number of contradictory policies apparent in the Administration's approach to the control of information. NSDD 145 provides that the Director of OMB is to review and amend as appropriate OMB Circular A-76 "Performance of Commercial Activities," and other OMB policies which pertain to national policy on telecommunications and automated information systems security. Yet on September 27, 1984, ten days after NSDD 145 was signed, OMB Deputy Director Joseph Wright announced that libraries and automated data processing were among the 14 categories of activities targeted for A-76 review throughout the federal government. As a result, several federal libraries have been turned over to the private sector for operation, and numerous federal libraries are currently under review for potential contracting out.

Contracting out can endanger national security either by eliminating altogether library expertise in the ranks of U. S. government workers or by releasing control of the government's information apparatus and databases to organizations which are components of or controlled by foreign interests. Nothing in Circular A-76 prohibits any nonfederal organization within or without the United States from bidding on an A-76 proposal. Therefore, nothing in A-76 would bar an organization of, for example, the Soviet Union from bidding on or even winning an A-76 contract to operate the library of the Department of State. There is a real and present danger that federal library contractors could use their positions to advance interests other than those of the government. Without question, in the course of running a federal library, A-76 contractors will acquire information about the agency and its programs. A contractor could use such information to undercut the competition when bidding on renewal or new contracts in the same agency.

ALA believes the Administration's position on this issue is untenable. Accordingly, last month ALA's Council passed a resolution urging Congress to declare a moratorium on all contracting out of federal libraries and document depositories and to hold further hearings on this matter. A copy of the resolution is attached to this statement.

Last year, at the behest of OMB, the National Technical and Information Service (NTIS) reviewed a number of alternatives for privatizing the agency. OMB announced its decision for the future of NTIS in one sentence in the Appendix to the Budget for fiscal 1988: "In 1988, the private sector will be offered the opportunity to operate NTIS on contract, with the government retaining overall policy direction." NTIS furnishes, among other things, a software clearinghouse and database support for agencies of the federal government as well as the nonfederal scientific and technical community. One of the agencies which receives direct, interactive database support from NTIS is the National Bureau of Standards. What happens to the security of NBS records if NTIS is contracted out to a foreign-owned firm?

ALA's concern about the repercussions of contracting out NTIS are expressed in still another attached resolution. This resolution states that "contracting out or privatization of NTIS could adversely affect equal and ready access to scientific and technical information crucial to the competitive position of the U. S. in the world economy and to the security of the nation." The resolution calls on Congress to "pass legislation...to assure that the interests of the American public...will not be vitiated should OMB proceed with its plan to contract out or privatize NTIS."

Concerns have also been expressed by social science researchers about foreign control of American information services. A recent report from the Social Science Research Council, Points of Leverage: An Agenda for a National Foundation for International Studies by Richard D. Lambert (New York, 1986) observes: "Yet we are almost absentmindedly allowing foreign concerns to gain control of some of the most important U.S.-based information services in the natural sciences;...." A few pages later the report states:

> There is a growing concern about the purchase by foreign firms of major American scientific information and distribution systems, which let them have immediate access to the products of our high-technology research without worrying about export restrictions.

The point we would like to emphasize is that all of these pieces are interrelated and, despite the Administration's attempts to have them viewed separately, they must be considered as part of a whole.

HR 145 will succeed only if the integrity and viability of the federal government's information infrastructure can be assured. If, in fact, those systems are controlled and operated by interests which could be inimical to the reliability of government information, then all the computer security standards ever devised will not suffice.

The picture that comes to mind, as a result of the current posture of the Administration is that of the American citizen, producing an identity card and lining up, with his or her tin cup, for a little milk from the Information Cow. Meanwhile, the halter around the neck of the cow trails out of the barn, across the pasture, and is firmly tethered, shall we say, in the Netherlands Antilles. We hope this analogy, comical but apt, can begin to produce on others the impression the current situation has produced among librarians.

In conclusion, we urge that this Subcommittee, as it considers HR 145, will also consider the effects of contracting out federal libraries and documents depositories as a part of the development of database security standards, and that a moratorium on such contracting out be put in place. We have tried---with virtually no success---to get OMB to understand the risks of contracting out federal libraries and document depositories. Possibly these hearings, and the obvious logical inconsistency between NSDD 145 and OMB Circular A-76 will finally get the point across.

On the one hand, internal government databases which should be protected are not; and on the other, databases which include publicly and widely available information are being speculatively scrutinized for possible restriction. This makes no sense at all. There ought to be some rational coordination of Administration programs affecting both the control and dissemination of government information. The American Library Association supports equal and ready public access to information generated by the federal government. We have always upheld the principle that American citizens, in fact citizens of all nations, should have wide access to information, and that the interchange of recorded information in all its forms between the United States and other countries is essential for international understanding. However, there is legitimate concern for national security in considering who controls government information.

Attachments

Resolution on "National Policy on Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems" (NTISSP No. 2, 29 October 1986)

WHEREAS, On October 29, 1986, the President's National Security Adviser issued an extremely broad new designation "sensitive but unclassified information" and directed federal government agencies to implement it; and

WHEREAS, On November 11, 1986, a senior Department of Defense official stated that privately owned unclassified electronic data bases would be reviewed for "sensitive but unclassified information" and that access to these data bases may be restricted or systems installed to monitor who uses them; and

WHEREAS, Over the last few months, representatives from the Department of Defense, Central Intelligence Agency and Federal Bureau of Investigation have been visiting private information companies to ask questions about who is using their information and for what purposes; and

WHEREAS, The institution of this new policy will restrict access to unclassified government and private sector information that has been easily and legally obtained by the public through libraries; and

WHEREAS, This Executive Branch Policy conflicts with American Library Association policy #53.4, Governmental Intimidation, and interpretation of the Library Bill of Rights:

> "The American Library Association opposes any use of government prerogatives which leads to the intimidation of the individual or the citizenry from the exercise of free expression;" and

WHEREAS, This Executive Branch Policy conflicts with American Library Association Policies regarding ready and equal access to government information, specifically:

Priority Area A. Access to information, in the American Library Association Priorities and Goals: "1) All individuals have equal access to libraries and information services," and "3) Government information in widely and easily available;" and

WHEREAS, The American Library Association policy #53.1, Library Bill of Rights states:

> "3) Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment," and

"5) A person's right to use a library should not be denied or abridged because of origin, age, background, or views;" now, therefore, be it

RESOLVED, That the American Library Association

1. Seek to have the "National Policy on Protection of Sensitive, But Unclassified Information In Federal Government Telecommunications and Automated Information Systems" repealed or rescinded;

2. Cooperate with other organizations to challenge the implementation of this policy, and;

3. Request the Freedom to Read Foundation to be alert to an appropriate opportunity to challenge the legality of this Policy.

Adopted by the Council of the
American Library Association
Chicago, Illinois
January 21, 1987
(Council Document #28)

Resolution on Foreign Control of Federal Libraries and Document Depositories

WHEREAS, The information resources of the federal government are vital to the security and economic well being of the United States; and

WHEREAS, Federal libraries and document depositories provide crucial support and unique resources for the development of policies, implementation of programs and ongoing operations of government agencies; and

WHEREAS, Federal libraries and librarians are key to effective utilization of these information resources, performing an inherently governmental function; and

WHEREAS, Federal libraries provide the longitudinal corporate memory of their agencies and their staffs, perform agency evaluations and actions under the Freedom of Information and Privacy Acts; and

WHEREAS, The American Library Association has opposed contracting out of federal libraries; and

WHEREAS, The Administration has expressed its concern regarding the sensitivity of certain types of federal information; and

WHEREAS, This Administration is using Office of Management and Budget Circular A-76 to force the contacting out to organizations outside the federal government of the information services provided by federal libraries and document depositories; and

WHEREAS, Circular A-76 does not restrict contracting for federal library and depository services only to United States firms and organizations; and

WHEREAS, At least one major departmental library and key functions in other federal libraries are already contracted out to U. S. subsidiaries of foreign firms; and

WHEREAS, It has been announced that a foreign owned firm is to be the successful bidder on another A-76 action which would allow this firm to take over the operation of a major scientific library in the federal government; now, therefore, be it

RESOLVED, That the American Library Association believes it is not in the best interest of the American people to contract out federal information programs and organizations to foreign owned or controlled firms; and, be it further

RESOLVED, That the American Library Association urge the Congress of the United States to declare a moratorium on all contracting out of federal

libraries and document depositories and to hold further hearings on this matter; and, be it further

RESOLVED, **That copies of this Resolution be transmitted to the President of the United States and his National Security Adviser, the President of the Senate, the Speaker of the House of Representatives, appropriate committees of the Congress, and the Director of the Office of Management and Budget.**

Adopted by the Council of the
American Library Association
Chicago, Illinois
January 21, 1987
(Council Document #26.7)

Resolution Concerning OMB's Proposed Privatization of NTIS

WHEREAS, The Office of Management and Budget (OMB) proposes to contract out or privatize the National Technical Information Service (NTIS); and

WHEREAS, Strong objections have been submitted to NTIS and OMB by the American Library Association, other professional library and information science associations, the academic and research community, individuals, and private sector organizations requiring rapid, economical access to scientific and technical information collected or generated with U. S. tax dollars; and

WHEREAS, ALA has expressed its concerns regarding the maintenance of the vital functions currently performed by NTIS, namely:

a) provision of a centralized source and permanent repository for a broad range of federal, international, state, local, and other unclassified scientific and technical reports;

b) provision of bibliographic access to the material through tools such as NTIS' Government Reports Announcements and Index;

c) dissemination of bibliographic information products of such a repository, i.e., catalogs, indexes, abstracts, and newsletters, through the Government Printing Office's Depository Library Program;

d) operation of a timely, "on demand" sales program for this scientific and technical information at prices affordable for not-for-profit libraries, educational institutions, students, small business entrepreneurs, and other similar groups; and

WHEREAS, Such contracting out or privatization of NTIS would adversely affect equal and ready access to scientific and technical information crucial to the competitive position of the U. S. in the world economy, and to the security of the nation; and

WHEREAS, The Office of Management and Budget has not responded publicly to these concerns; now, therefore, be it

RESOLVED, That the American Library Association calls upon the Congress of the United States to hold hearings on OMB's proposal and, if necessary, draft and pass legislation designed to assure that the interests of the American public and the functions identified above will not be vitiated should OMB proceed with its plan to contract out or privatize NTIS; and, be it further

RESOLVED, That copies of the Resolution be transmitted to the President of the Senate, the Speaker of the House of Representatives, appropriate committees of Congress, the Secretary of Commerce, the Director of the National Technical Information Service, and the Director of the Office of Management and Budget.

Adopted by the Council of the
American Library Association
Chicago, Illinois
January 21, 1987
(Council Document #26.6)